User Manual
Admin Report Kit for Active Directory

Admin Report Kit for Active Directory
ARKAD
Copyright (c) 2006-2014 Vyapin Software Systems Private Limited. All Rights Reserved.
Email: support@vyapin.com Web: www.vyapin.com

Last Updated: July 2014

Copyright © 2006-2014 Vyapin Software Systems Private Ltd. All rights reserved.

This document is being furnished by Vyapin Software Systems Private Ltd for information purposes only to licensed users of the ARKAD software product and is furnished on an “AS IS” basis, that is, without any warranties, whatsoever, express or implied. *ARKAD* is a trademark of Vyapin Software Systems Private Ltd. Information in this document is subject to change without notice and does not represent any commitment on the part of Vyapin Software Systems Private Ltd. The software described in this document is furnished under a license agreement. The software may be used only in accordance with the terms of that license agreement. It is against the law to copy or use the software except as specifically allowed in that license. No part of this document may be reproduced or retransmitted in any form or by any means, whether electronically or mechanically, including, but not limited to the way of: photocopying, recording, or information recording and retrieval systems, without the express written permission of Vyapin Software Systems Private Ltd.

Vyapin Software Systems Private Limited

Website: http://www.vyapin.com/
Sales Contact: sales@vyapin.com
Technical Support: support@vyapin.com

Table of Contents

1 About Admin Report Kit for Active Directory (ARKAD) _____ 1

1.1 System requirements _____ 5

1.2 Who can use ARKAD? _____ 5

1.3 How to Activate the Software? _____ 6

1.4 Technical Support _____ 8

2 How to use ARKAD effectively? _____ 9

2.1 Configure Directory Server _____ 9

2.2 Launch Connection Manager _____ 9

2.3 How to Add Server to Connection Manager? _____ 11

2.4 How to Edit Server in Connection Manager? _____ 14

2.5 How to Delete Server in Connection Manger? _____ 16

2.6 How to View Properties of Server in Connection Manager? _____ 17

2.7 How to Find Data in a Report? _____ 18

2.8 How to Export Data? _____ 20

2.9 How to E-mail data? _____ 21

2.10 How to refresh data? _____ 25

2.11 How to Add/Remove Columns? _____ 25

2.12 How to Use Advanced Filter? _____ 27

2.13 How to use Quick Filter? _____ 31

2.14 How to read the Report Status label? _____ 33

2.15 How to Configure SMTP Server? _____ 35

2.16 How to Configure Profile Manager? _____ 36

3 Object Reports (Working with Reports) _____ 38

3.1 How to view Domain Reports? _____ 38

3.2 How to view Sites Reports? _____ 44

3.3 How to view Organizational Unit Reports ____ 48

3.4 How to view Computer Accounts Reports? ____ 54

3.5 How to view Users Reports? ____ 60

3.6 How to view Groups Reports? ____ 69

3.7 How to view Contacts Reports? ____ 74

3.8 How to view Foreign Security Principals? ____ 79

3.9 How to view RSoP Reports? ____ 83

3.10 How to view Group Policy Object Reports? ____ 90

3.11 How to view Starter GPOs Reports? ____ 95

3.12 How to view WMI Filter Reports? ____ 97

3.13 How to view Password Settings Objects Reports? ____ 100

4 Quick Reports ____ 105

4.1 About Quick Reports ____ 105

4.2 How to generate Quick Reports? ____ 106

5 Built-in Reports ____ 107

5.1 About Built-in Reports ____ 107

5.2 How to Generate Built-in Object Reports? ____ 108

5.3 How to Generate Built-in Security Reports? ____ 111

6 Forest Reports ____ 117

6.1 About Forest Reports ____ 117

6.2 How to generate Forest Reports? ____ 117

7 Permissions Reports ____ 120

7.1 About Permissions Reports ____ 120

7.2 How to create Permissions Reports? ____ 120

7.3 How to generate Permissions Reports? ____ 129

7.4 How to Manage Permissions Reports? ____ 132

8 Custom Reports _____ *135*

8.1 About Custom Reports _____ 135

8.2 How to create Custom Reports? _____ 135

8.3 How to generate Custom Reports? _____ 142

8.4 How to Manage Custom Reports? _____ 145

9 Custom LDAP Query Reports _____ *148*

9.1 About Custom LDAP Queries _____ 148

9.2 How to Create Custom LDAP Query Report? _____ 148

9.3 How to Generate Custom LDAP Query Report? _____ 154

9.4 How to Manage Custom LDAP Query Report? _____ 155

9.5 How to Delete Custom LDAP Query Report? _____ 156

10 AD Summary Reports _____ *157*

10.1 About AD Summary Reports _____ 157

10.2 How to generate AD Summary Reports? _____ 157

11 Insight Reports _____ *161*

11.1 About Insight Reports _____ 161

11.2 How to view Insight Report for Organizational Units? _____ 162

11.3 How to view Insight Report for Computer Accounts? _____ 166

11.4 How to view Insight Report for Users? _____ 171

11.5 How to view Insight Report for Groups? _____ 177

12 Power Search _____ *182*

12.1 About Power Search _____ 182

12.2 How to Perform a New Power Search? _____ 184

12.3 How to Manage Power Search Reports? _____ 192

12.4 How to Generate Power Search Reports? _____ 196

12.5 How to Perform a New Account Search? _____ 197

13 How to generate Terminal Services Reports? 200

13.1 About Terminal Services Reports 200

13.2 How to generate Terminal Services Reports? 200

14 Power Export 202

14.1 About Power Export 202

14.2 Scheduled Tasks Manager 204

14.3 Schedule Object Reports 206

14.4 Schedule Built-in Object Reports 211

14.5 Schedule Built-in Security Reports 217

14.6 Schedule Forest Reports 224

14.7 Schedule Permissions Reports 229

14.8 Schedule Custom Reports 234

14.9 Schedule Custom LDAP Queries Reports 239

14.10 Schedule AD Summary Reports 244

14.11 Schedule Quick Reports 250

14.12 Schedule Terminal Services Reports 256

15 Compare Reports 261

15.1 How to Compare Reports? 261

16 References 263

16.1 Troubleshooting 263

16.2 How to Uninstall ARKAD? 264

17 Index 267

Chapter 1

1 About Admin Report Kit for Active Directory (ARKAD)

Admin Report Kit for Active Directory (ARKAD) is a powerful reporting tool for the Microsoft Active Directory Enterprise. ARKAD collects configuration information about various objects and their properties in the Active Directory and reports them in a simple but elegant format for System Administrators and IT Infrastructure Managers.

About ARKAD Editions In the evaluation period, there is no restriction in features. You can test all the features available in ARKAD. The only restriction is that you can export/ e-mail the first 10 records only. The evaluation period is 15 days.

The evaluation version will work as an advanced edition.

ARKAD comes in two versions: Standard and Advanced edition. The following table describes the differences between them.

Feature Name	Feature Description	Standard Edition	Advanced Edition
List of Reports			
Object Reports	Reports about objects and their properties in Active Directory like **Users, Groups, OU, GPO etc.,**	√	√
Quick Reports	Provides a quick and consistent way for administrators to retrieve specific attributes information from a Active Directory Domain. **E.g. Disabled User Accounts.**	√	√
Permissions Reports	User-defined reports for viewing permissions assigned to specific accounts on objects in the directory.	√	√

Forest Reports	Allows the user to generate forest-wide reports for Users, Groups etc. **e.g. Users 'Member of' details for all domains in a forest.**	**X**	√
Custom Reports	Allows the users to create their own custom reports (user-defined) by combining different sections of an Object Report). **e.g. List of all User with their name, e-mail, manager, company, Title, logon name, mobile no, address details, Account details etc.,**	**X**	√
Custom LDAP Queries	Allows the user to create their own Quick Reports to search only the specified domain partition, and searches can be narrowed down to a single container/OU object. Users can also specify their own **LDAP** queries	**X**	√
AD Summary Reports	Provides overall summary information about a single Active Directory domain. **E.g. Total no of users, Groups, Computers in a Domain / Organizational Units.**	**X**	√
Built-in object Reports	Provides complex parameterized reports. **E.g. Users who have NOT logged on recently based on a date-range value (From 10/01/2010 To 10/31/2010).**	**X**	√
Built-in Security Reports	Provides pre-defined Security/Auditing reports.	**X**	√
Insight Reports	Reports Summary and Detailed information based on "frequency of occurrence (Counts)" of objects and their attributes, **e.g. "Number of recently created objects in a given time period".**	**X**	√

Power Search	Facilitates searching of selected permission(s) over Active Directory objects like Users, Groups, Contacts, Computers, Organizational units and Domain Controllers. **e.g. "who can change passwords of users in a domain"**	X	√
Terminal Services Reports	Reports about Terminal Services or Remote Desktop Services information of roaming users in a domain.	X	√
Compare Reports	Compares the reports generated using ARKAD and presents the difference between them.	X	√
Scheduled Report			
Power Export	Allows the user to select multiple reports and run these reports against different domains at scheduled intervals. The scheduler supports several different scheduling options. The Power Export supports Export / E-mail delivery options in different file formats at scheduled intervals.	X	√
Delivery Options			
Export	Helps the user to export report data generated by ARKAD to a file using various formats namely HTML / CSV / XLSX.	√	√

E-mail	Provides the option to e-mail the reports generated.	X	√
Filters			
Quick Filter	Allows you to view a narrow subset of data by specifying a filter condition that could either be applied to any of the fields or to a specific field in the current report.	√	√
Add/Remove Columns	Add/Remove columns can be created with the desired set of fields that are related to a given report.	√	√
Find	Provides the option to search for specific data in a report.	√	√
Advanced Filter	Allows you to filter report data based on compound and complex filter conditions. Also gives the user the ability to create filter conditions that include one or more fields in the report and is also capable of reporting fields with empty values in the report.	X	√

1.1 System requirements

For the computers running by ARKAD

Hardware: Intel Pentium III or higher processor, 512 MB of RAM, 30 MB disk

Operating System: Windows 8.1 / Windows 8 / Windows 7 / Windows Vista / Windows XP / Windows Server 2003 / Windows Server 2008 / Windows Server 2008 R2 / Windows Server 2012 / Windows Server 2012 R2 with .NET Framework 4.0 with the latest service packs.

Software: MDAC

For the computers reported by ARKAD

Windows Server 2012 R2 / Windows Server 2012 / Windows Server 2008 R2 / Windows Server 2008 / Windows 2003 (SP2) running Active Directory. Please refer to question #8 in FAQ for more information.

1.2 Who can use ARKAD?

Any company having Windows 2012 / Windows 2008 / 2003 Active Directory servers

Users that would benefit from ARKAD

- Systems management personnel
- System Administrators
- Other Windows network product developers
- Trainers and educators
- Enterprise network planning personnel

Organizations that would benefit from ARKAD

- Companies having Microsoft Enterprise Network based on Active Directory
- Any company having Windows 2012 / 2008 / 2003 Active Directory servers

1.3 How to Activate the Software?

Once you purchase the software online or through any one of our resellers, you will receive a sale notification through e-mail from our sales department. We will send you an e-mail with the necessary instructions to activate the software.

In case you do not receive an e-mail from our sales team after you purchase the software, please send the following information to our sales department at sales@vyapin.com with the sales order number:

- **Company Name:** End-user Company Name
- **Location:** City & Country for the Company Name given above

Please allow 12 to 24 hours from the time of purchase for our sales department to process your orders.

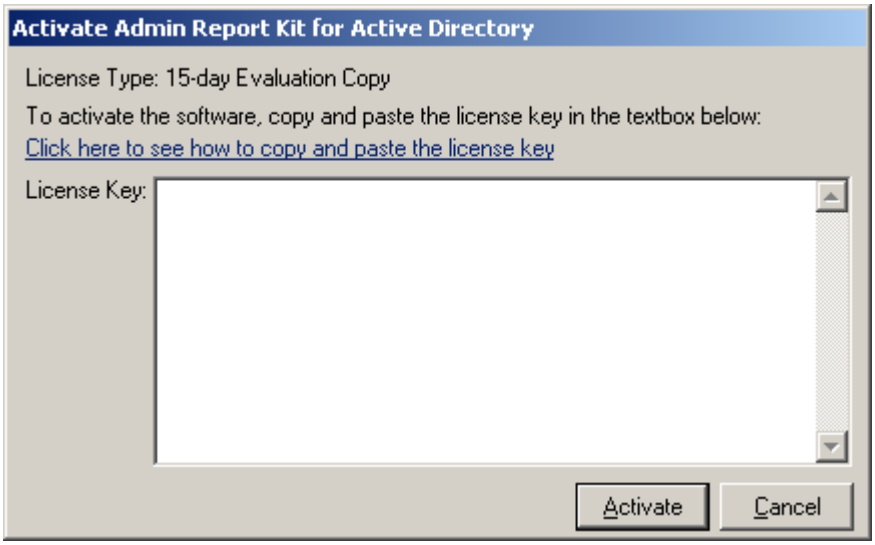

Activate Admin Report Kit for Active Directory
License Type: 15-day Evaluation Copy
To activate the software, copy and paste the license key in the textbox below:
Click here to see how to copy and paste the license key
License Key:
Activate
Cancel

Image 1 - Activate screens

Perform the following steps to activate the software:

1) Download evaluation/trial copy of software from the respective product page available in our website at http://www.vyapin.com/

2) Install the software on the desired computer.

3) You will receive a license key through e-mail as soon as the purchase process is complete.

4) Click *'Activate' in Help -> About* -> Activate menu to see the Activate dialog (as shown in Image 1).

5) Copy the *license key* sent to you through email, and pastes it in the 'License Key' textbox. For help on how to copy the license key, click 'Click here to see how to copy and paste the license key' link in the Activate dialog (as shown in Image 2).

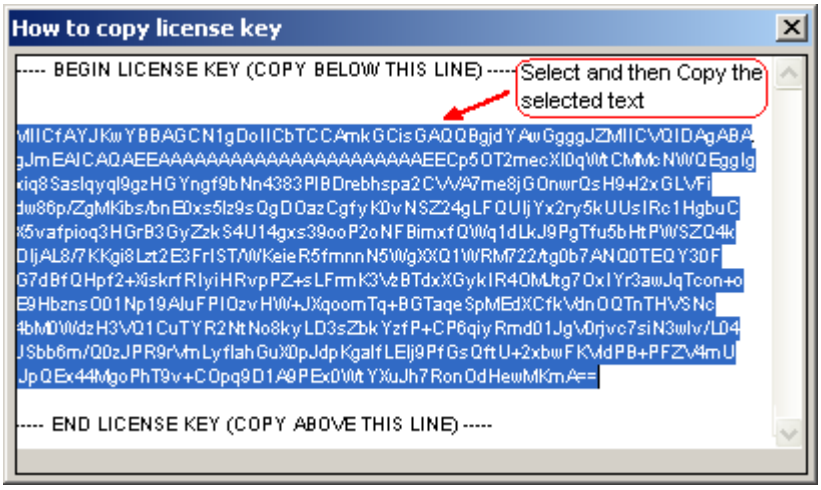

How to copy license key
----- BEGIN LICENSE KEY (COPY BELOW THIS LINE) -----
Select and then Copy the selected text
----- END LICENSE KEY (COPY ABOVE THIS LINE) -----

Image 2 - How to copy license key screen

1.4 Technical Support

ARKAD Frequently Asked Questions (FAQ) section is available online at our website http://www.vyapin.com.

Please direct all technical support questions to support@vyapin.com. Include the following information to expedite a response:

a) Include the version of the product you are using.
b) If the problem is associated with installation, include the steps that led to the problem.
c) If the problem is associated with usage, please state the series of steps you performed.
d) Include the version of the OS, info about any service packs or hot-fixes and local language of the OS installed.
e) Attach the Error Log File - E.g., <Application Data Folder>\ARKAD 8.x\ARKADErrorLog.log

NOTE:

<Application Data Folder> is the common area where ARKAD settings will be stored in the computer running ARKAD. The path will be as follows:

a) Windows XP, Windows 2003 - C:\Documents and Settings\All Users\Documents
b) Windows 8, Windows 7, Windows Vista, Windows 2008, windows 2012 - C:\Users\Public\Documents

Chapter 2

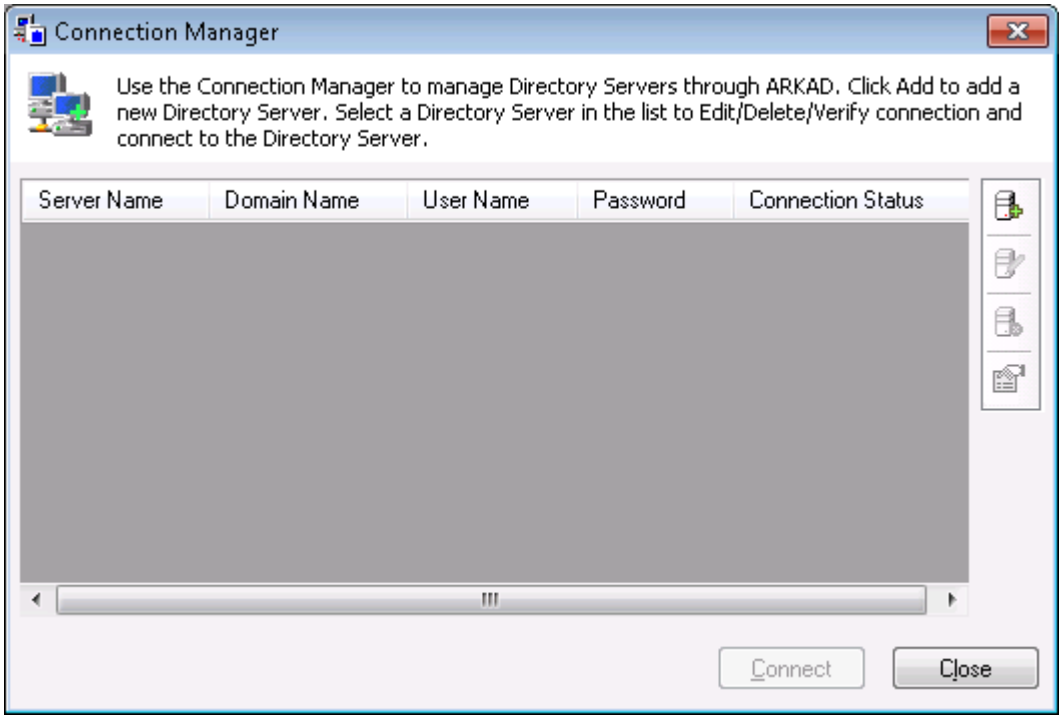
2 How to use ARKAD effectively?

2.1 Configure Directory Server

The Connection Manager maintains a list of Directory Servers that can be managed through ARKAD. Using the Connection Manager window, you can add/edit/delete the directory Servers and connect to the available directory servers to generate reports.

2.2 Launch Connection Manager

You can launch ARKAD Connection Manager:


Connection Manager
Use the Connection Manager to manage Directory Servers through ARKAD. Click Add to add a new Directory Server. Select a Directory Server in the list to Edit/Delete/Verify connection and connect to the Directory Server.
Server Name
Domain Name
User Name
Password
Connection Status
Connect
Close

The various operations that can be performed in the Connection Manager are given below:

Operation	Description
Add	To Add a Directory Server to the server list.
Edit	To Edit the properties of the Directory Server in the server list. Select a Directory Server and click Edit button.
Delete	To Delete a Directory Server from the server list. Select a Directory Server and click Delete button.
View Properties	To view the properties of the Directory Server in the list. Select a Directory Server and click Properties button.
Connect	To connect to the Directory Server in the list and launch the report window. Select a Directory Server and click Connect button.
Close	To close the Connection Manager window. Click Close button.

2.3 How to Add Server to Connection Manager?

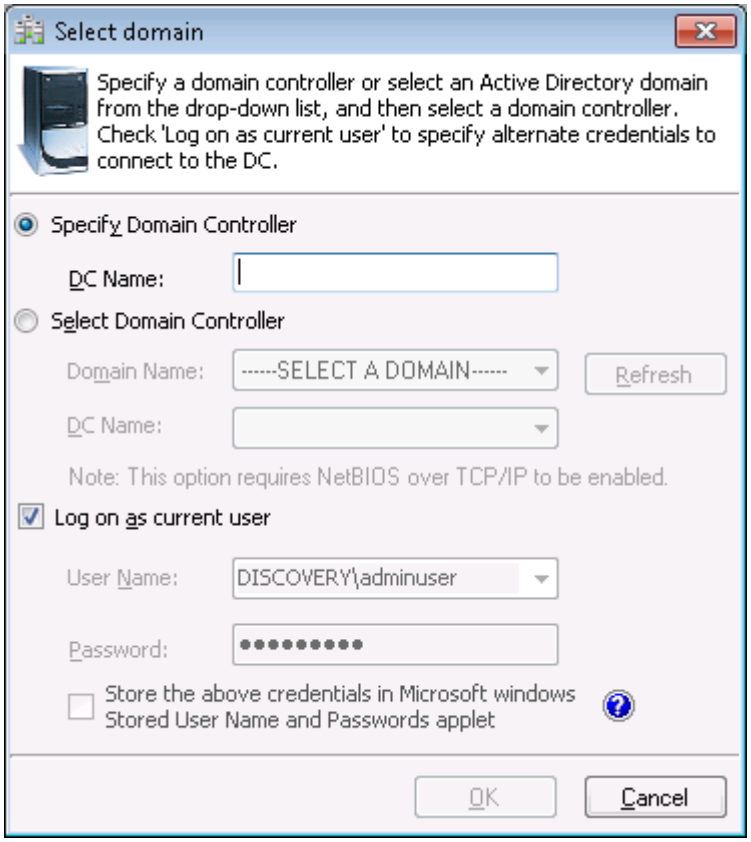
Add a Directory Server

You have to specify the directory server information for adding a directory server in ARKAD

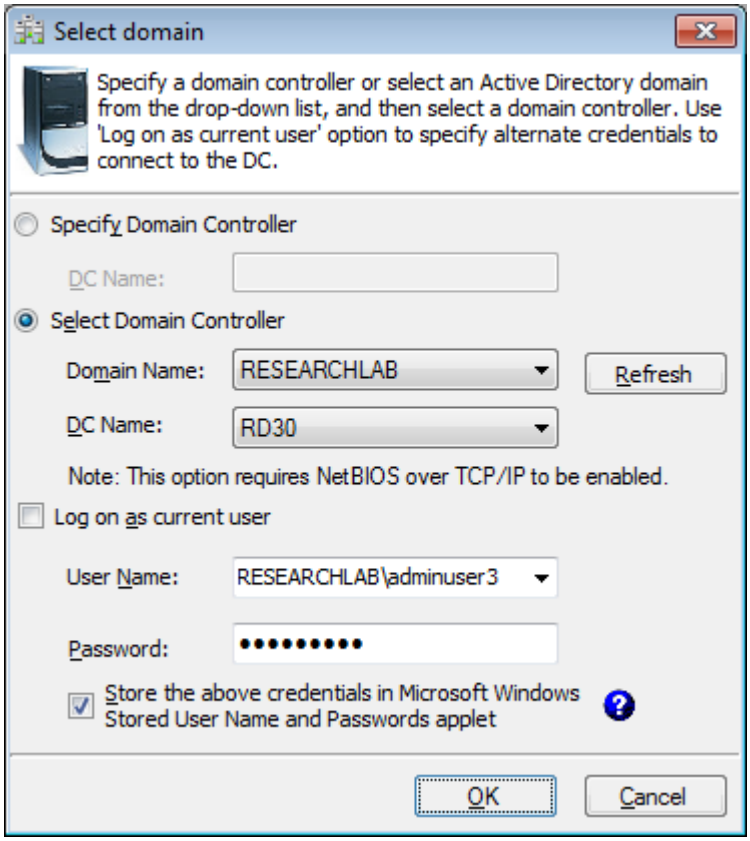
Directory Server - This section contains the information required to connect to the Active Directory Server (Domain Controller

Add a Directory Server to the list

1) Launch **Connection Manager** Window.
2) In the Connection Manager window, click Add button to add a Directory Server to the list.
3) The New Directory Server window will be displayed as shown below:


Select domain
Specify a domain controller or select an Active Directory domain from the drop-down list, and then select a domain controller.
Check 'Log on as current user' to specify alternate credentials to connect to the DC.
Specify Domain Controller
DC Name:
Select Domain Controller
Domain Name:
-----SELECT A DOMAIN-----
Refresh
DC Name:
Note: This option requires NetBIOS over TCP/IP to be enabled.
Log on as current user
User Name:
DISCOVERY\adminuser
Password:
Store the above credentials in Microsoft windows Stored User Name and Passwords applet
OK
Cancel

- The list of domains available in the network will be loaded in the Domain Name dropdown.
- **Select a domain** from the Domain Name dropdown.
- The list of domain controllers for the selected domain will be loaded in the *Domain Controller Name* dropdown.
- **Select a domain controller** from the *Domain Controller Name* dropdown.


Select domain
Specify a domain controller or select an Active Directory domain from the drop-down list, and then select a domain controller. Use 'Log on as current user' option to specify alternate credentials to connect to the DC.
Specify Domain Controller
DC Name:
Select Domain Controller
Domain Name:
RESEARCHLAB
Refresh
DC Name:
RD30
Note: This option requires NetBIOS over TCP/IP to be enabled.
Log on as current user
User Name:
RESEARCHLAB\adminuser3
Password:
Store the above credentials in Microsoft Windows Stored User Name and Passwords applet
OK
Cancel

4) Specify **user name** and the corresponding password to connect to the specified server.

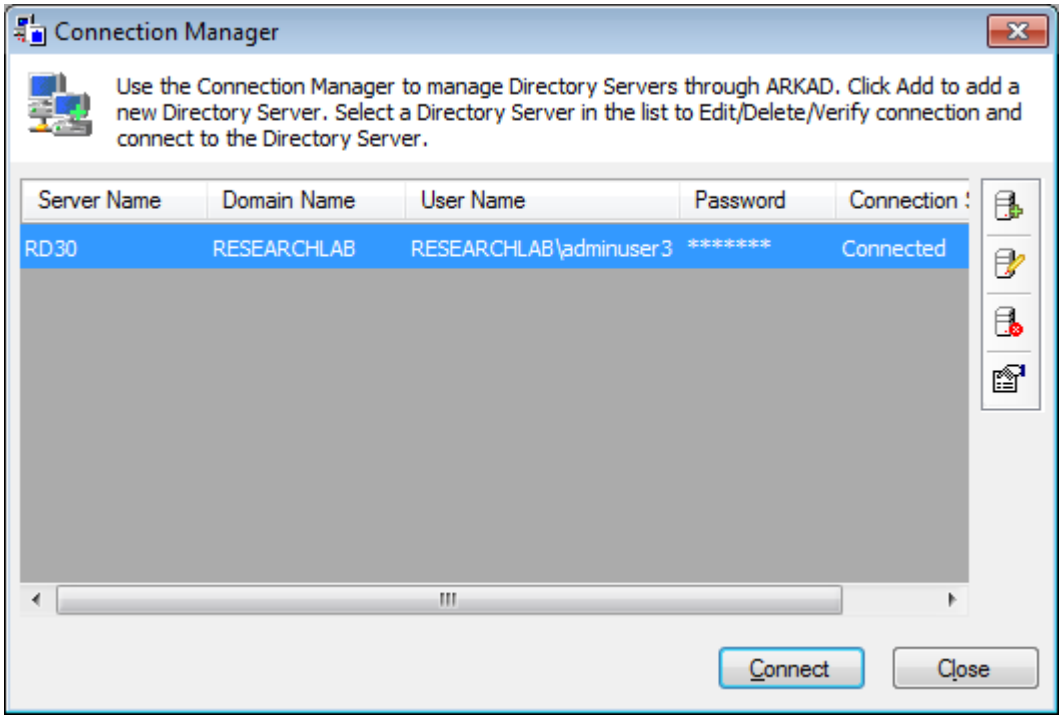
Store the above user credential in Microsoft Windows Stored User Names and Passwords applet - In Built-in and Power Reports, ARKAD allows the user to enter different user credentials to connect to the Directory Server. Select the checkbox if you like to connect to the directory server using a different user context and to create a scheduled report task (unattended mode).

By default, ARKAD will use the user account specified in the scheduled 'Run As' user context to connect to Directory Server in Power Reports tool. In case, if you decide to use different user context to connect to Directory Server when running the scheduled task, you can do so by storing the Directory Server user context for future use.

ARKAD will store the user credential to connect to Directory Server in the Microsoft Windows Stored User Names and Passwords applet for security reasons. The stored user profile is tied to the user context (currently logged on user account) in which the profile is created. Hence, you will not be allowed to change the scheduled 'Run As' user context for the import task.

5) Click **OK** to add the Directory Server to the *Connection Manager* list.

6) ARKAD will connect to the Directory Server with the newly provided connection parameters and add it to the list, upon successful connection to the Directory Server.



7) Click **Cancel** to abort the add process of the Directory Server to the Connection Manager list.

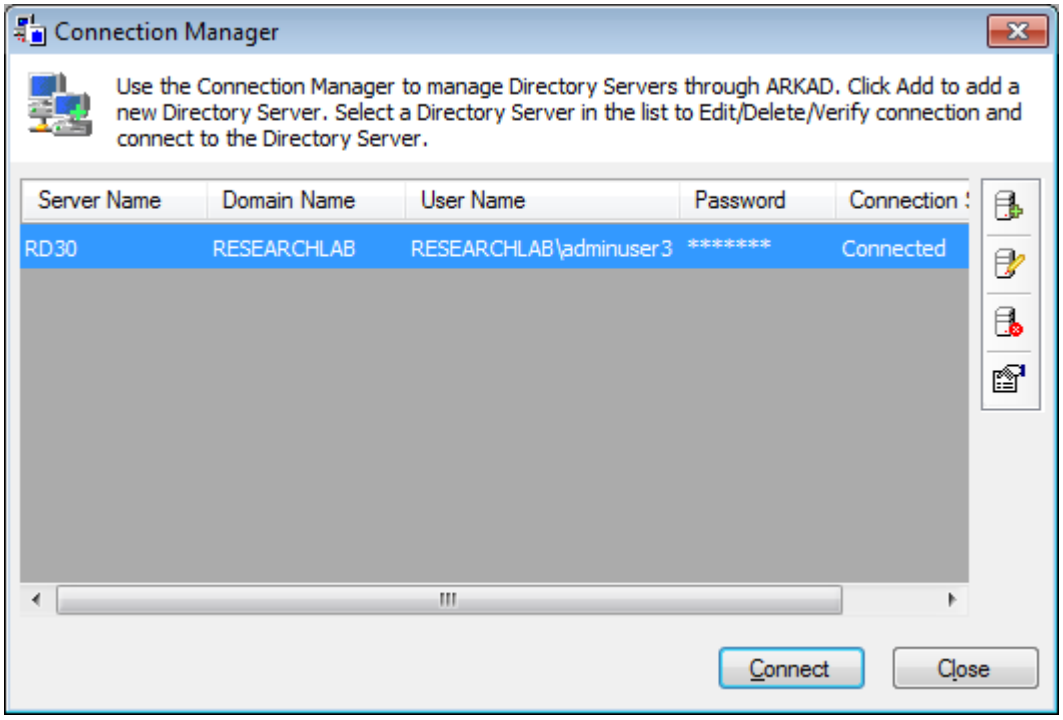
2.4 How to Edit Server in Connection Manager?

Edit a Directory Server

To Edit a Directory Server listing in the Connection Manager, follow the steps given below:

1) Launch Connection Manager Window.

2) In the Connection Manager window, select any row (Directory Server), **Click Edit** button to Edit an existing Directory Server in the list, as shown below:

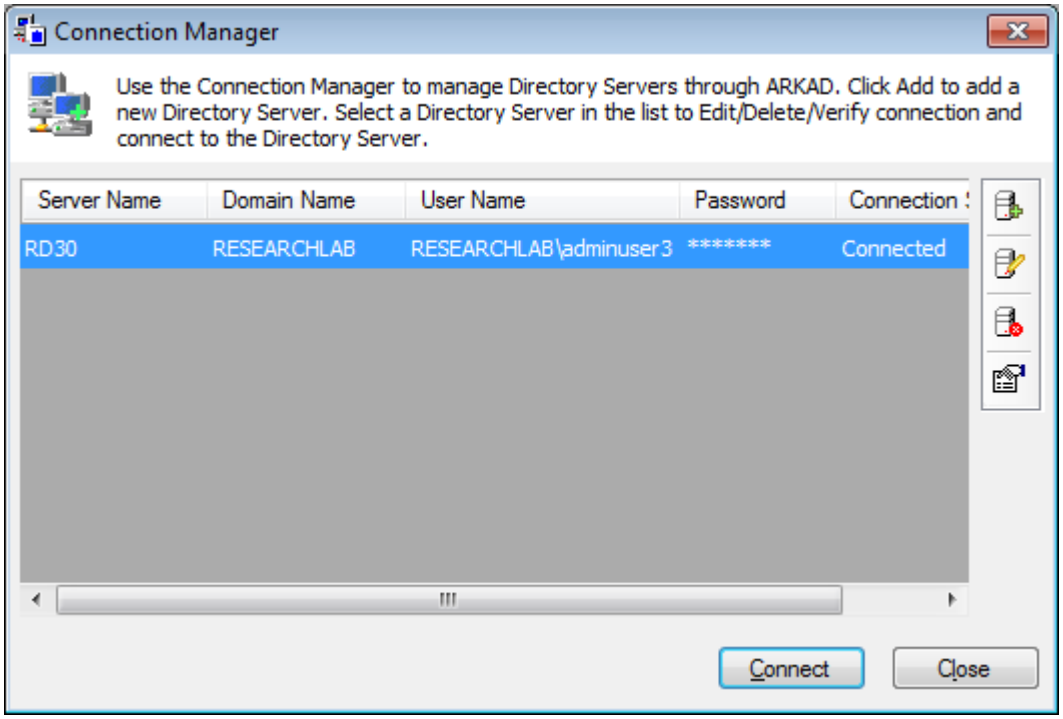


3) The Directory Server Name cannot be modified during the edit operation.

4) Specify *user name* and the corresponding *password* to connect to the specified server.

5) Click **OK** to save and connect to the Directory Server with the newly provided connection parameters and update the Directory Server in the Connection Manager list.

6) ARKAD will connect to the Directory Server with the newly provided connection parameters and modify it in the list, upon successful connection to the Directory Server.



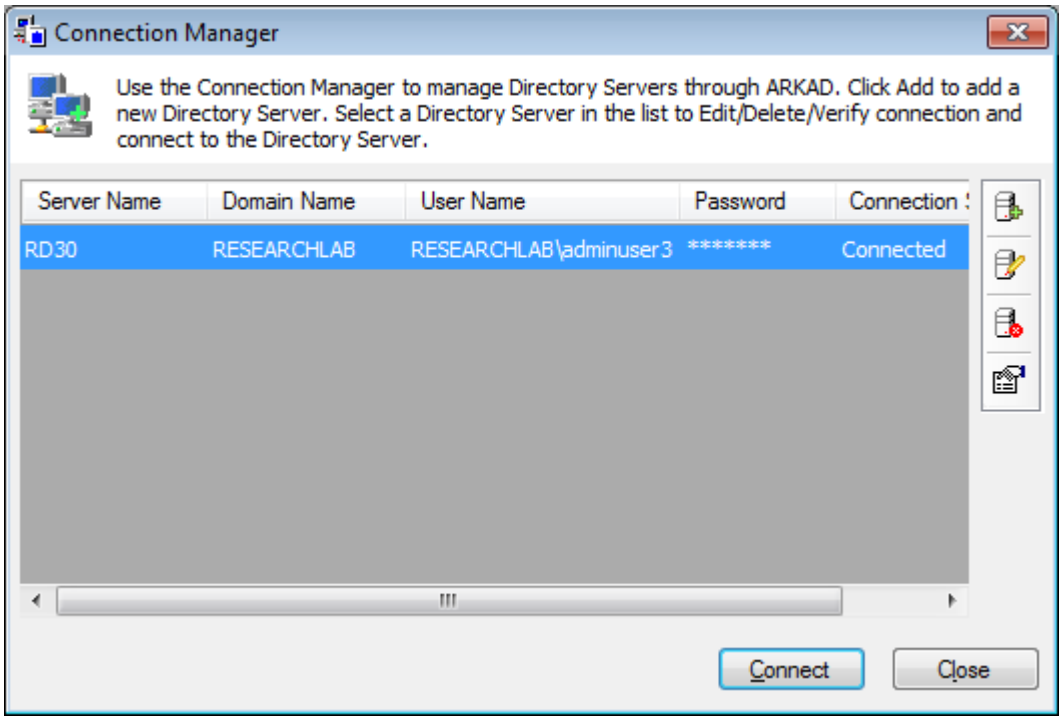
7) Click Cancel to retain the existing connection parameters of the Directory Server in the Connection Manager list.

2.5 How to Delete Server in Connection Manger?

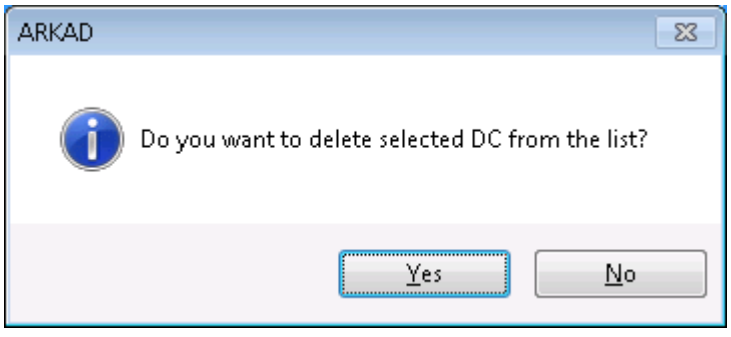
Delete a Directory Server

Perform the following steps to delete a Directory Server Launch **Connection Manager** Window.

1) In the Connection Manager window, select any row (Directory Server), click **Delete** button to delete the Directory Server from the Connection Manager list.



2) An **alert message** asking for confirmation to delete the Directory Server will be displayed as shown below:



4) *Click* **yes** to delete the selected Directory Server.

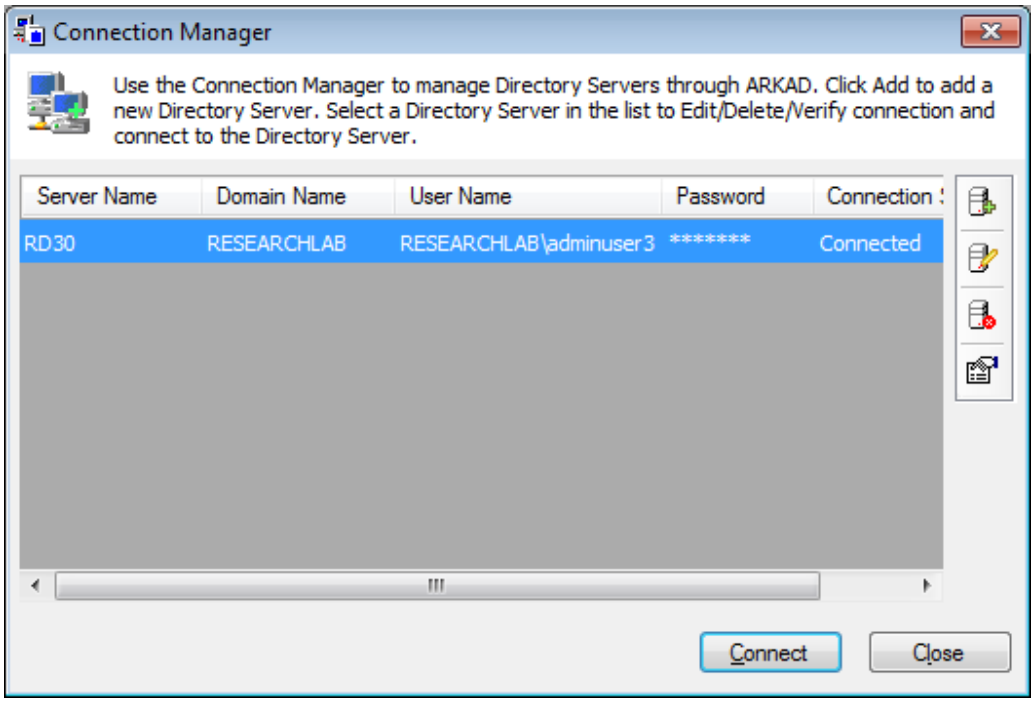
5) *Click* **No** to abort the delete process of the selected Directory Server.

2.6 How to View Properties of Server in Connection Manager?

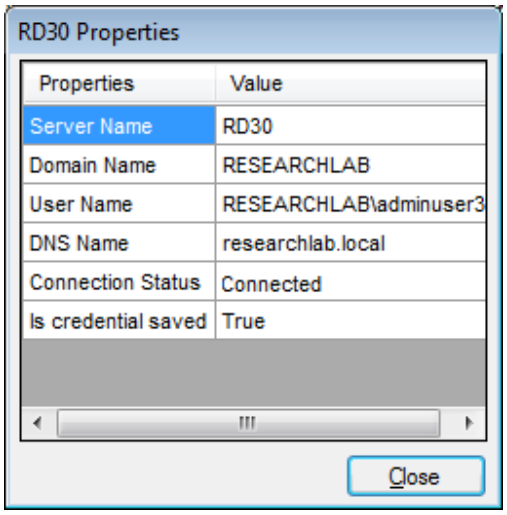
View properties of Directory Server

Perform the following steps to view properties of Directory Server:

1) Launch **Connection Manager** Window.
2) In the Connection Manager window, select any row (Directory Server), click **Properties** button to view the properties of the selected Directory Server from the Connection Manager list.



3) The *property* window with the selected Directory Server information *(Server Name, Domain Name, User Name, DNS Name, Connection Status, Is credentia Saved)* will be displayed as shown below:



2.7 How to Find Data in a Report?

You can use the find feature in ARKAD to search for specific data in a report.

To search for data in a report, just type the characters or words you want to find in the find edit box, available in the report window, and then click on.

NOTE: You can use the "*" wildcard character in the search criteria. The "*" wildcard character act as a place holder for zero or more characters. However, note that you cannot use the "?" wildcard character in the search criteria.

For instance, if you want to search for 'Domain' in a report. Type Domain, without quotations, in the edit box, and then click on Find Button.

NOTE*:* The search criteria should not be enclosed within quotation marks.

NOTE*:* ARKAD performs a case insensitive search of the specified search criteria in the report.

By default, ARKAD adds an asterisk as a suffix to the specified search criteria, if no wildcard characters were present in it. In this case, ARKAD finds a match in the report for all fields that have the text Domain followed by zero or more characters, that is, Domain, Domain Controllers, and Domain Admins etcetera.

For all the matches found, ARKAD highlights the corresponding columns in the grid, and scrolls the grid automatically to the first occurrence.

NOTE*:* ARKAD finds additional occurrences of the specified search criteria instantaneously. To locate other occurrences of the same search criteria in a report you need to scroll the report grid downwards.

The following table summarizes the behaviour of the find feature:

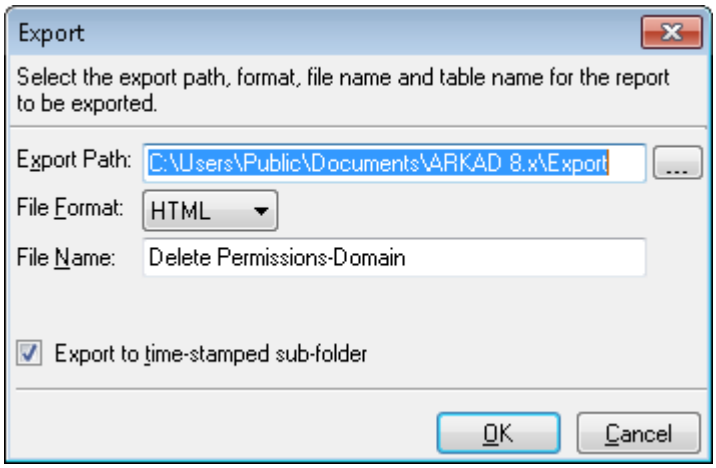
Search Criteria	Description
Domain	Searches the report for **domain** followed by zero or more characters. For instance, domain, domain admins etc.
*Users	Searches the report for **users** starting with zero or more characters and ending with users. For instance, users, mobile users etc.
User	Searches the report for **user** starting with zero or more characters and ending with zero or more characters. For instance, user template, backup user etc.

2.8 How to Export Data?

The **Export** feature helps the user to export report data generated by ARKAD to a file using various formats namely HTML/CSV/XLSX.

Click on

button in the report window or select **Export** option under **File** menu to export report data to a file in the desired format.



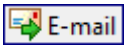
Specify a file name to export report data to or accept the default file name. Specify the export path and select a desired file format. The path refers to the destination location where the output file generated should be stored. It can be given using the Browse button. To avoid overwrite existing files, if any, in the specified export path, By default, the report will be exported to a time-stamped sub-folder, in the format 'YYYY-MM-DD HH.MM.SS', under the specified export path.

In **CSV** file format, the information is stored as comma separated values. For each report, a CSV file will be generated. The name of the CSV file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared or under a sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path if "Export to time-stamped folder" option is set.

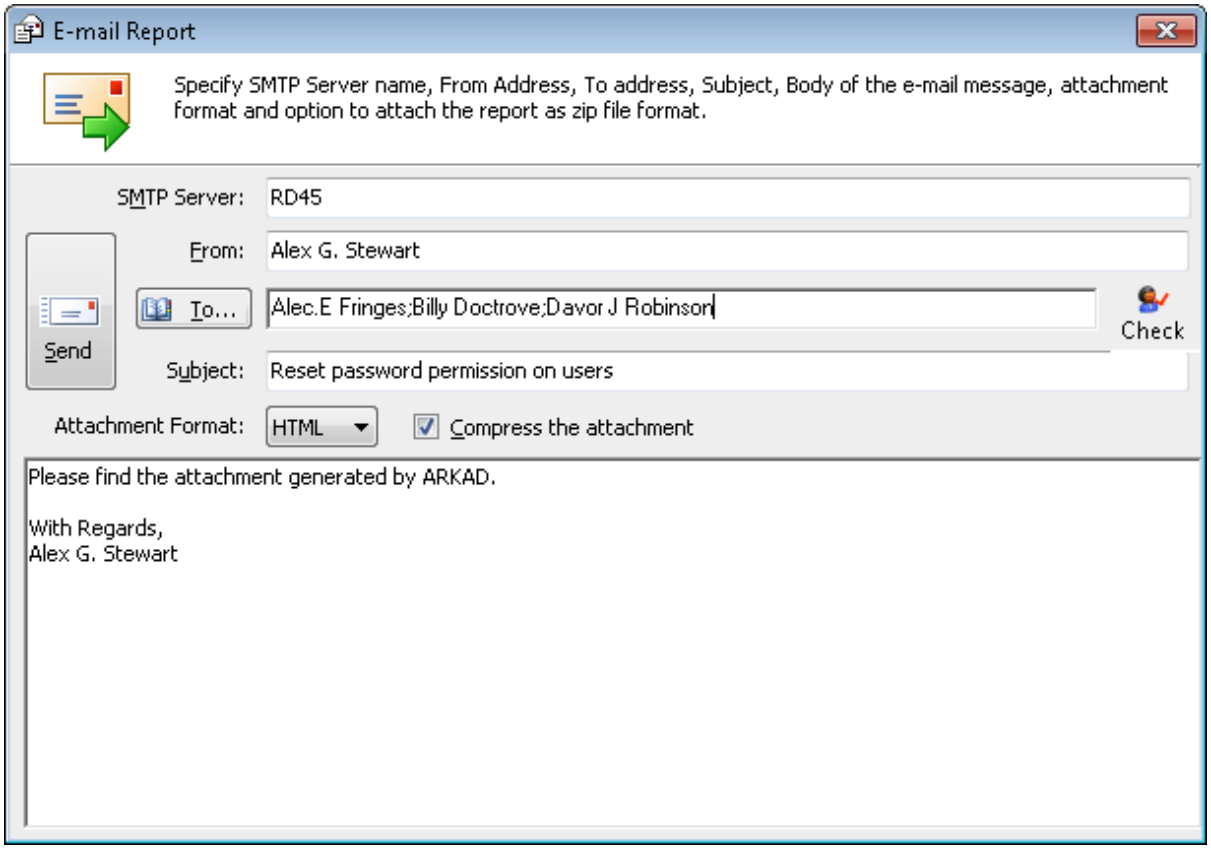
In **HTML and XLSX** file format, the information is stored in the html and xlsx file respectively. For each report, a HTML file will be generated. The name of the HTML file will be the name of the report and is stored in the specified destination path if "Export to time-stamped folder" option is cleared or under a sub-folder, of the form YYYY-MM-DD HH.MM.SS, under the specified export path if "Export to time-stamped folder" option is set.

2.9 How to E-mail data?

ARKAD provides the option to e-mail the reports generated.

Click 

button in the toolbar to e-mail the report to e-mail recipients. E-mail dialog will be displayed as shown below:



For e-mailing reports, ARKAD requires *SMTP Server*, From E-mail Address, To E-mail Addresses (recipients separated by semicolon) and the report attachment format.

Specify SMTP server name, from Address, To Address, mail subject, mail content, attachment format and option to compress the attachment.

Click

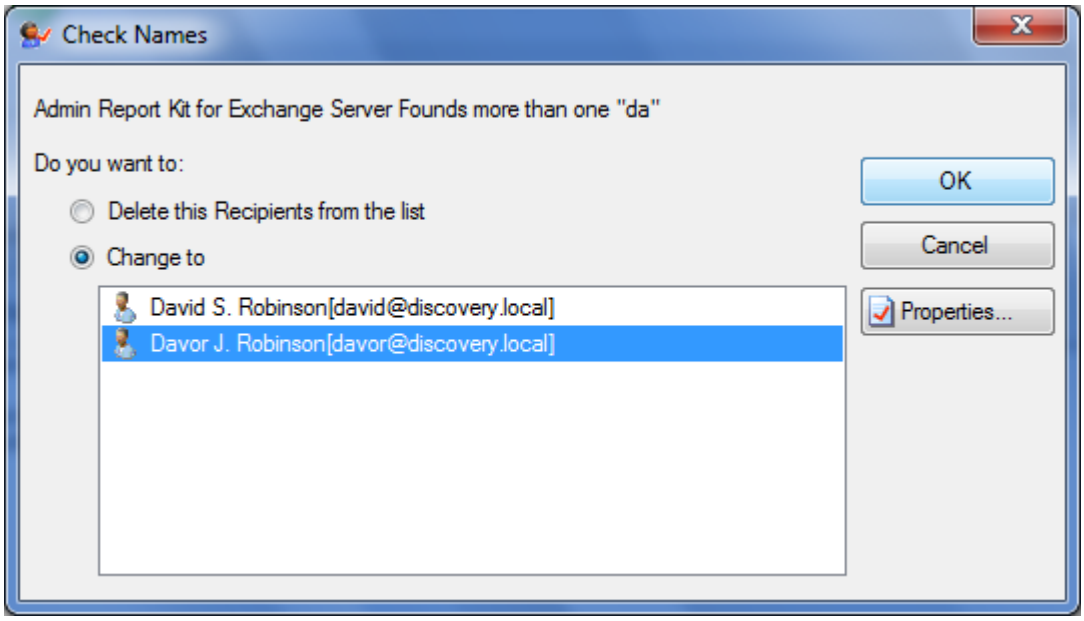
button to send the report by e-mail to the selected recipients.

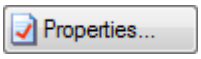
Check names

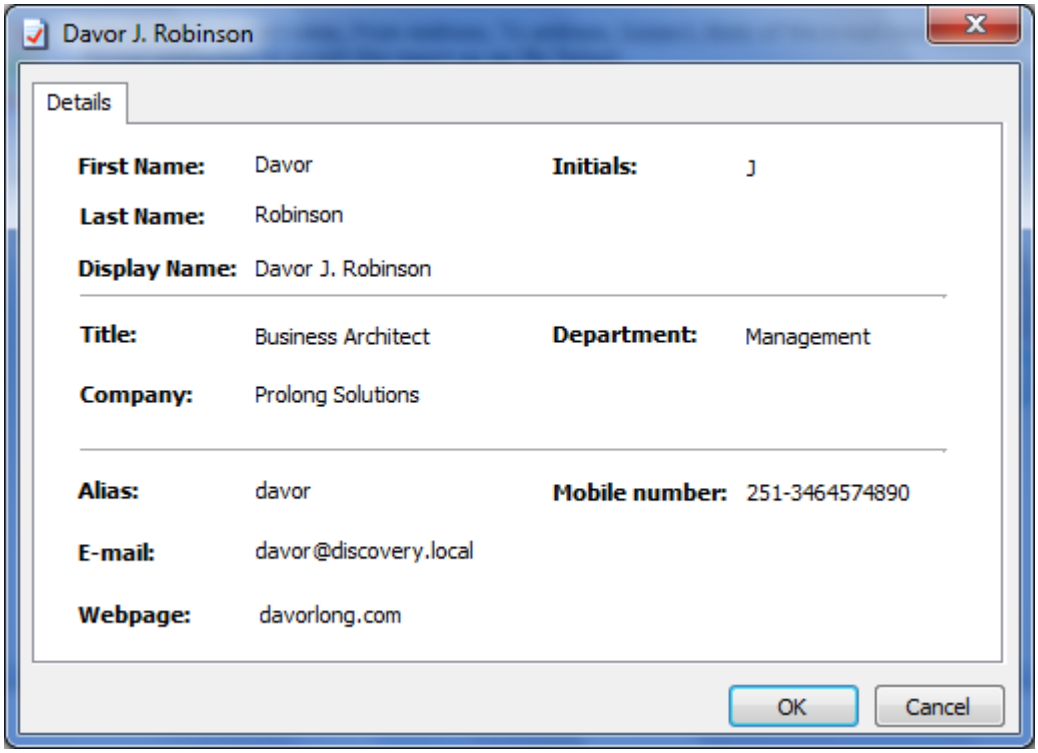
ARKAD provides check name feature to check the existence of corresponding mail-enabled recipient object in Active Directory. To check name, **click**

button. If the

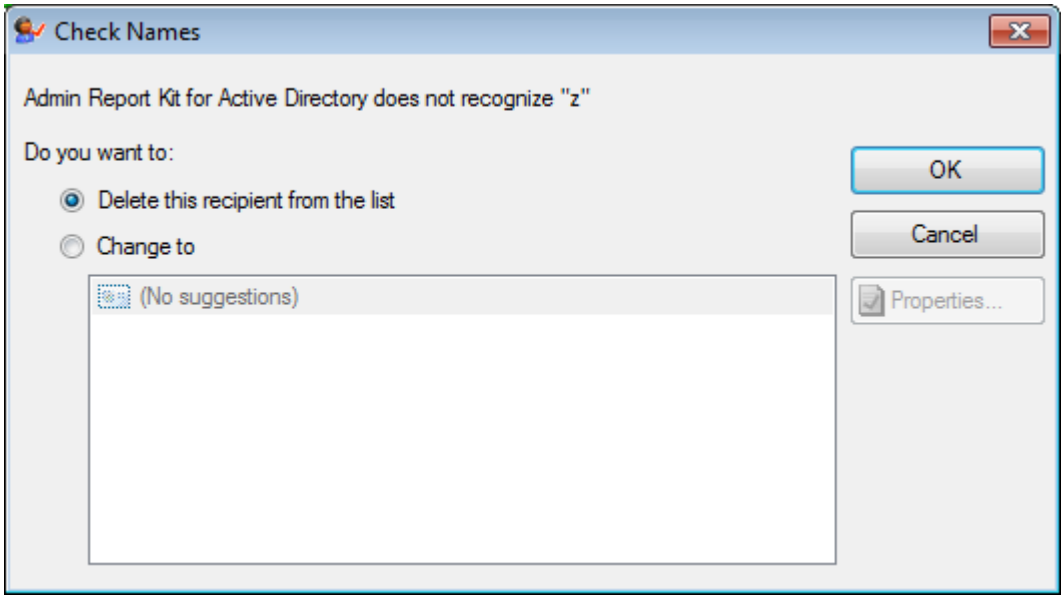
entered name matches with a mail object in the Active directory / its trusted domain, name entered in From Address textbox will be replaced by the corresponding active directory recipient object. If there is more than one match, a dialog which contains matching Active Directory recipients will appear as shown below. You can select one or more recipient and click **OK.**



- To get more information about the listed recipients under **Change to**, select the name, and then **click** 

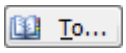


If there is no match for the name entered by the user in Active Directory, a dialog will appear as shown below:

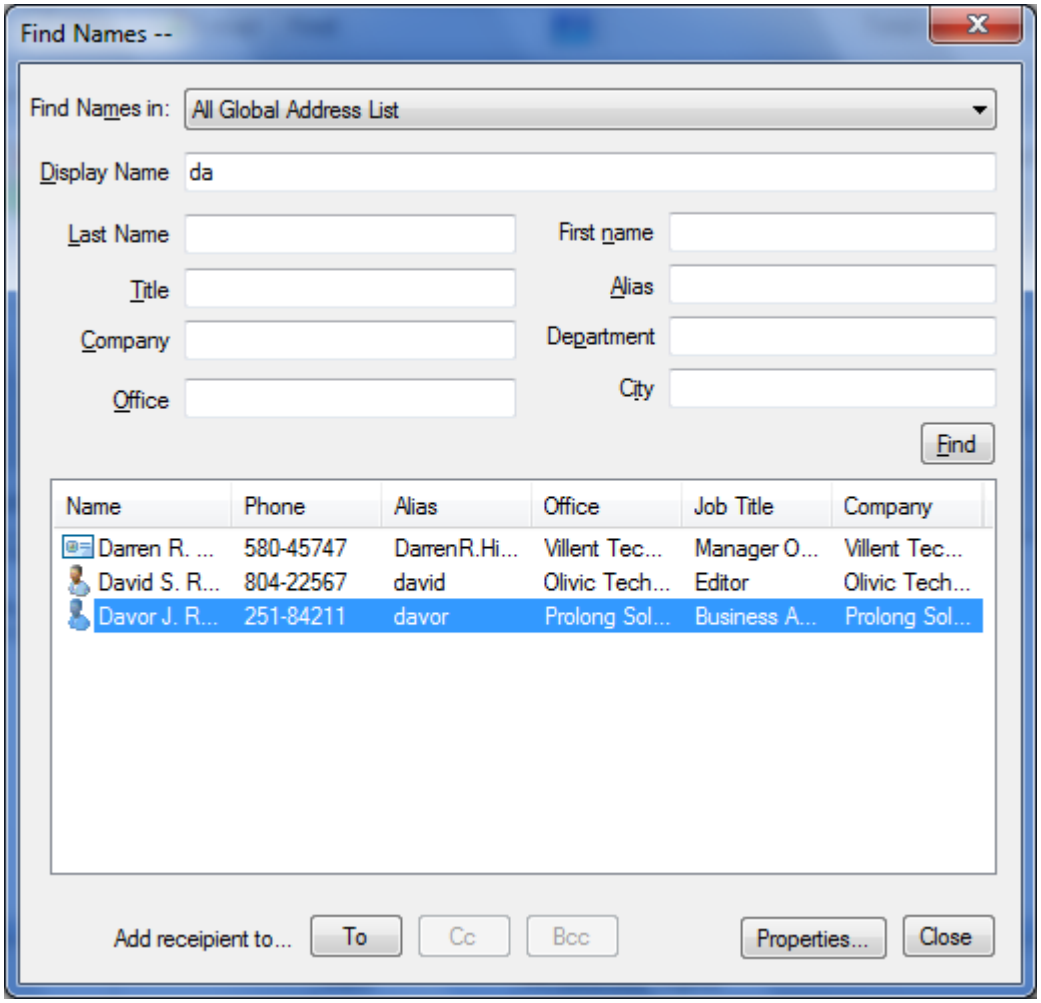


Select Delete option in the above dialog to *remove* the recipient name from To Address text box Click Cancel button to close this dialog and the unresolved recipient(s) will appear in **red** colour.

Address Book

ARKAD provides Address Book feature to search for any mail enabled recipient object (say, person, distribution list, contact, public folder) you want to send a message to. **Click** 

button and then use the **Find Names** dialog box to search for the recipient object you want to send a message to. (Note that you can't use the **Find Names dialog** box to search for distribution lists in your Contacts folder.) Select the object's name in the list and then click **Add recipient to...To.**



- To get more information about one of the names in the list, such as department or phone number, select the name, and then click

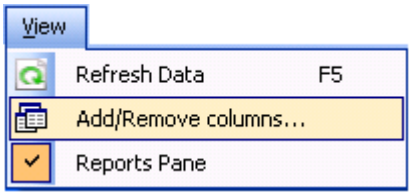
2.10 How to refresh data?

Refresh the current report data to view the latest information from the Domain Controller.

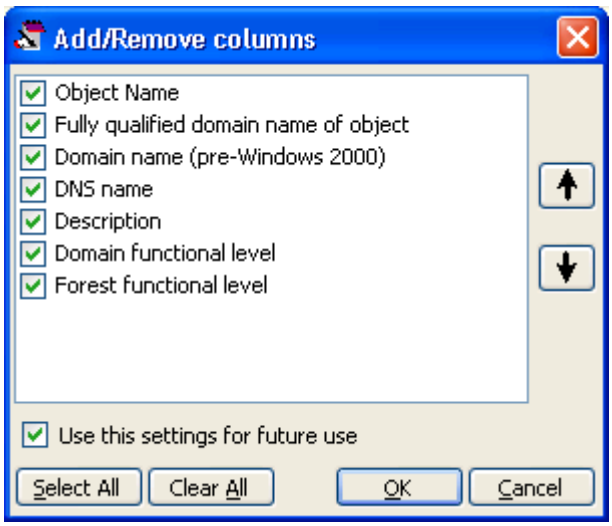
Click On

button in the toolbar available in the report window or press F5 to refresh *report data*. Alternatively, you can right-click on the grid, in the right pane of the report window, and then select *'Refresh Data'* from the context menu. The existing data will be cleared and latest data will be loaded in the report window.

2.11 How to Add/Remove Columns?

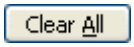
Click on 

to **Add/Remove Columns**



Click

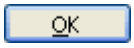
for **selecting** all the check boxes.

Click 

for **clearing** all the check boxes.

You can use the arrow buttons to order the fields. To move a field up by one position in the list of fields click button. To move a field down by one position in the list of fields click button

You can retain Add/Remove columns settings for future use by selecting 'Use this setting for future use' checkbox

Click  button for **confirming** the changes.

Click button for **cancelling** the operation.

2.12 How to Use Advanced Filter?

Advanced Filter tool allows you to filter report data based on compound and complex filter conditions. Unlike Quick Filter, Advanced Filter gives the user the ability to create filter conditions that include one or more fields in the report and is also capable of reporting fields with empty values in the report.

ARKAD allows for complete filter management for advanced filters. You can create new filters, edit existing ones to suit your needs and delete unwanted filters.

The Advanced Filter tool is available just below the report grid in the right pane as shown below:

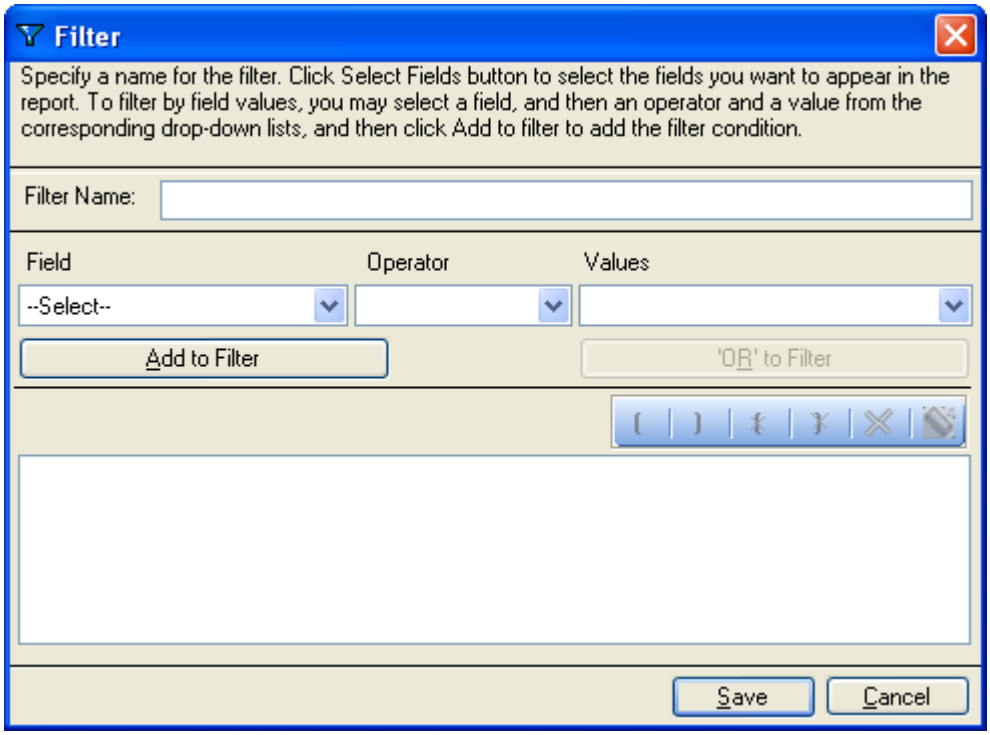
To apply a filter to the current report, select the filter from the Advanced Filters drop-down and click on button.

To remove a filter applied to the current report, select **No Filter Applied** from the *Advanced Filters* drop-down and click on button.

Create a new filter

Click on to create a new advanced filter for the current report

The ***Filter*** window will appear as shown below:


Filter
Specify a name for the filter. Click Select Fields button to select the fields you want to appear in the report. To filter by field values, you may select a field, and then an operator and a value from the corresponding drop-down lists, and then click Add to filter to add the filter condition.
Filter Name:
Field
Operator
Values
--Select--
Add to Filter
'OR' to Filter
Save
Cancel

To set a filter condition, follow these steps.

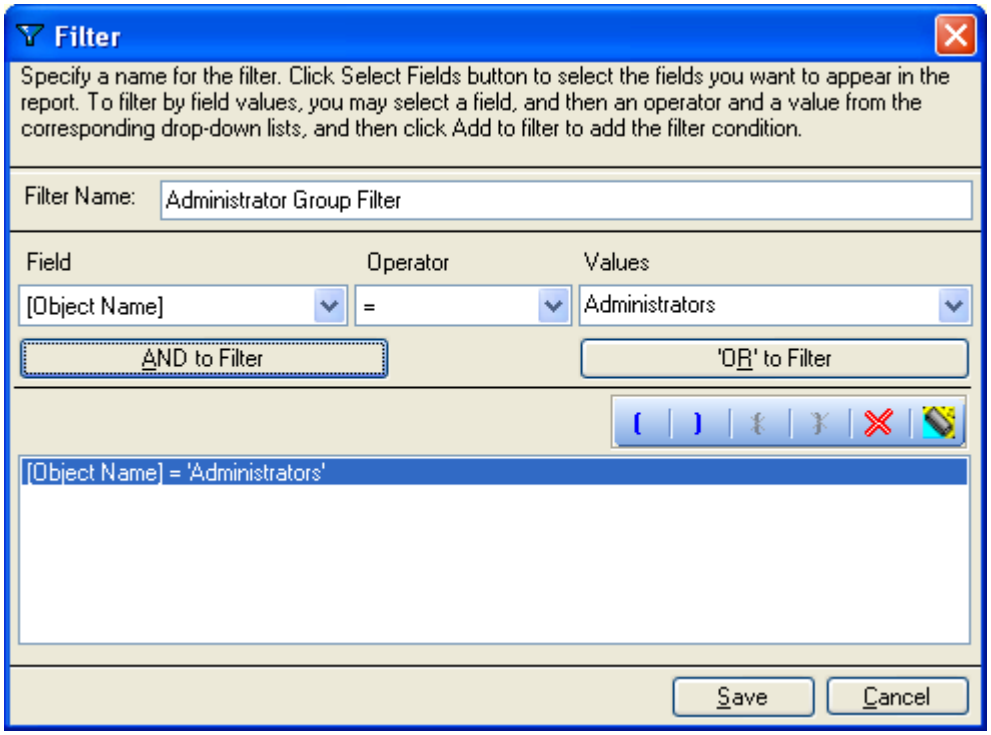
1) Specify a **name** for the filter.

2) *Click* on button to select the fields you want to appear in the report. However, this step is optional. ARKAD, by default, displays all the fields of the report if you choose not to select specific fields of the report.

3) **Choose** a **field name**, an **operator** and a possible **value** from the respective drop-down lists.

4) *Click* to add the *filter condition.*

5) Then the **Add to Filter** button will change to **AND to Filter** and **OR to Filter** button will be enabled. The selected condition will be added as shown below.


Filter
Specify a name for the filter. Click Select Fields button to select the fields you want to appear in the report. To filter by field values, you may select a field, and then an operator and a value from the corresponding drop-down lists, and then click Add to filter to add the filter condition.
Filter Name:
Administrator Group Filter
Field
Operator
Values
[Object Name]
=
Administrators
AND to Filter
'OR' to Filter
( ) { } X
[Object Name] = 'Administrators'
Save
Cancel

6) *Click* **Save** to apply the filter to the current report. Also, the filter will be saved to the filter database, for later use. You can select a filter from the advanced filters drop-down list and apply it to a report.

The report status label, just above the grid, shows the filter status **"Filter:"** that indicates whether the current report is filtered or not.

For a **normal view**, the *filter status* will appear as

For a **filtered view**, the *filter status* will appear as

NOTE:

- *Click* to *clear* all the filter conditions in the list.
- Use

and

to build enhanced filter condition as shown below:
- (Field A = Value 1 AND Field B = Value 2) OR (Field C = Value 3 AND Field D = Value 4)
- Use to *remove* the parenthesis
- Use to *delete* a condition from the list of filter conditions. This will *remove* the currently selected filter condition from the list.

Edit an existing filter

To edit an existing saved filter, select the filter from the advanced filters drop-down list, and then click on button. The filter window will appear on the screen. You may edit the fields-list and filter conditions. Also, you can choose to save the filter in a different name, retaining the original filter, or overwrite the existing filter with the new filter conditions and fields-list.

You can also edit the built-in filters provided in the application. However, once you overwrite a built-in filter with a new fields-list and/or filter conditions, you will loose the original built-in filter. So, it is advisable to save the modified built-in filter to a different name, which will allow you to retain the original filter and have a customized version of the filter that suits your needs.

Delete an existing filter

To *delete* an existing filter*, select* the *filter* from the advanced filters drop-down list and click on button.

However, if the filter, that you had deleted, had been applied to a report, ARKAD removes the filter from being applied to that report, and then deletes the selected filter.

***NOTE**:* Built-in filters provided by ARKAD cannot be deleted.

2.13 How to use Quick Filter?

The Quick Filter allows you to view a narrow subset of data by specifying a filter condition that could either be applied to any of the fields or to a specific field in the current report.

The *Quick Filter* tool is available just below the report grid in the right pane as shown below:

Apply Filter

To *filter report data*, follow these steps:

1) **Select a field** from the field's drop-down list. Instead, if you want to apply the filter condition to any of the fields in the current report, select **"Any Field"** from the field's drop-down list.
2) **Select an operator** from the operators' drop-down list, beside fields drop-down.
3) **Type** in a filter condition in the edit box, beside operator's drop-down list.

NOTE: You can use **wildcard characters** such as "*" and "?" in the filter condition.

The *filter condition* can include regular characters as well as wildcard characters as given below:

Filter Condition	Description	Example
a*	Character starting with a	[Object Name] = a* finds object name beginning with a, for example ARKAD, Administrator, and so on.
a?	Character starting with a and maximum of two characters including a	[Object Name] = a? Finds object name that has only two characters, starting with a, for example AD and so on.
a?d*	Minimum of three characters, the first character being a, middle character may be any single character and the last character being d	[Object Name] = a?d* finds object name beginning with a, that has any single character in the middle and ending with d followed by zero or more characters.

Click on to *apply* the filter condition.

Remove Filter

To **remove** the **quick filter** that had already been applied to the current report, click on button.

2.14 How to read the Report Status label?

ARKAD displays a *report status label* (just above the grid in the right pane of the report window) where you can see the following information in the specified order:

1) Report generation time-stamp
2) Report status
3) Filter status

The *report status* label is shown below:

The report status label consists of three panes as mentioned earlier.

Report generation time-stamp

The first pane shows the date and time on which the report was last generated in the format dd MMM, yyyy hh:mm:ss AM/PM. This time-stamp information will help you identify if the report contains latest domain information.

Report status

The second pane in the *report status* label shows the *status of the report* collection process.

The following table shows the *possible messages* that might be displayed in this pane:

Status message	Meaning
Completed	Report collection completed successfully without any error(s)
Completed with errors (see note)	Report collection was completed. However, some errors were encountered during data collection.
Cancelled	Report collection was cancelled. No errors were encountered during data collection.
Cancelled with errors (see note)	The report collection was cancelled and some errors were encountered during data collection.

Error	The report collection was aborted and report data was not collected. This can happen if ARKAD determines that target domain controller does not meet necessary system requirements criteria for a given report. For instance, all RSoP reports require the target domain controller to be running Windows 2003 Server.
Not Collected	The report collection was aborted due to an unrecoverable error, and as a result, the report data was not collected. This can happen if one or more files that ARKAD depends on are missing or are not registered properly.

NOTE: The report status pane switches to a hyper link when error(s) occur during data collection. You can click on this pane (second pane) to view error(s) that were encountered during the previous data collection.

Filter status

The third pane in the report status label shows whether any filter has been applied, or otherwise, to the current report. This filter status pane applies to both Quick Filter and Advanced Filter tools.

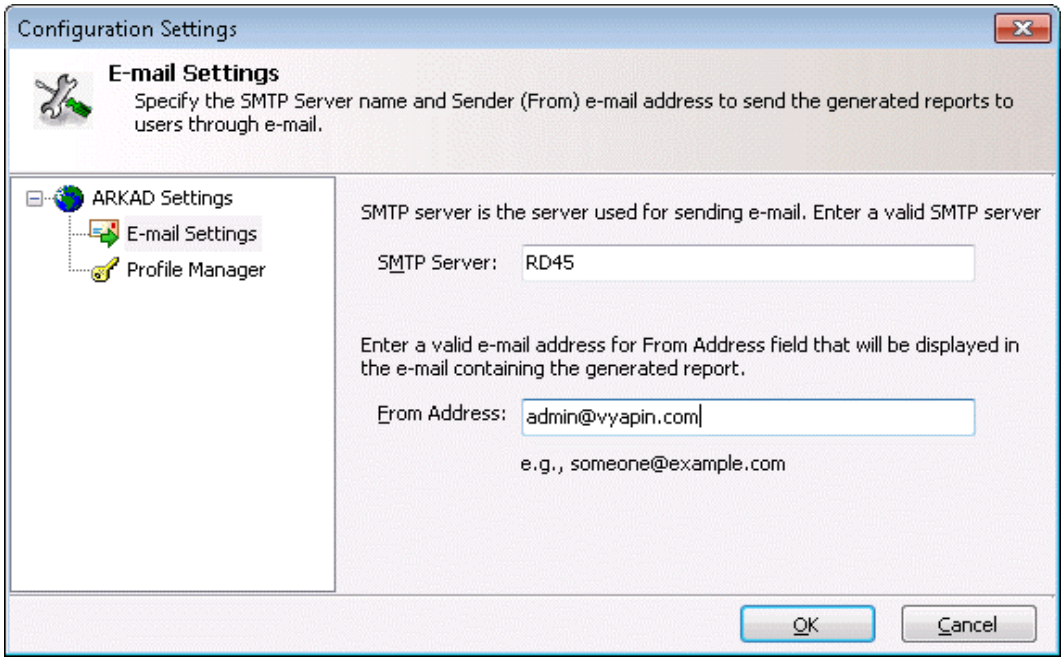
The following table shows the *possible messages* that might be displayed in this pane:

Status Message	Meaning
Not Applied	No filter (both Quick Filter and Advanced Filer) has been applied to the current report. Therefore the report data is not filtered.
Applied	A filter (either Quick Filter or an Advanced Filter) has been applied to the current report. Therefore the report data is filtered.

2.15 How to Configure SMTP Server?

ARKAD provides the option to e-mail the reports generated using Power Reports tasks. For e-mailing reports, ARKAD requires SMTP Server, From E-mail Address, To E-mail Addresses (recipients separated by semicolon) and the e-mail report format. ARKAD maintains a single SMTP Server and a From E-mail Address for use by all Power Report tasks. You can specify a separate set of To e-mail Addresses (recipients), e-mail report format, subject and body of the message for each Power Report task.

You can set *SMTP Server* and From Address by clicking *Tools -> Configuration Settings* menu in the *ARKAD main application* window, as shown below:


Configuration Settings
E-mail Settings
Specify the SMTP Server name and Sender (From) e-mail address to send the generated reports to users through e-mail.
ARKAD Settings
E-mail Settings
Profile Manager
SMTP server is the server used for sending e-mail. Enter a valid SMTP server
SMTP Server:
RD45
Enter a valid e-mail address for From Address field that will be displayed in the e-mail containing the generated report.
From Address:
admin@vyapin.com
e.g., someone@example.com
OK
Cancel

2.16 How to Configure Profile Manager?

Profile Manager

ARKAD creates a user profile in **Windows Stored User Names and Passwords** applet, and *Directory Server* user context for report generation using *Built-in Reports* and *Power Reports* feature.

The stored user profile will be useful for generating reports using ARKAD under the following scenarios:

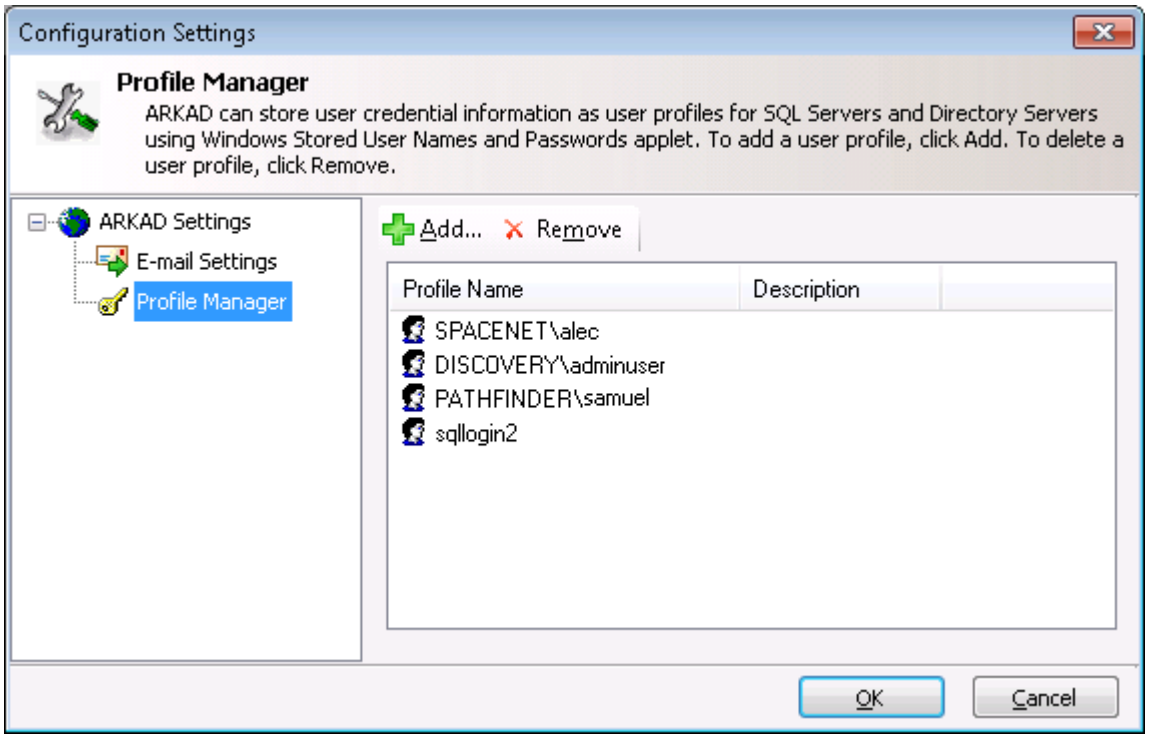
- Using an *alternate user account* to connect to the *Directory Server.*

The stored user profile persists for all subsequent logon sessions on the same computer where ARKAD is installed. The stored user profiles are visible to the application under other logon sessions on the same computer.

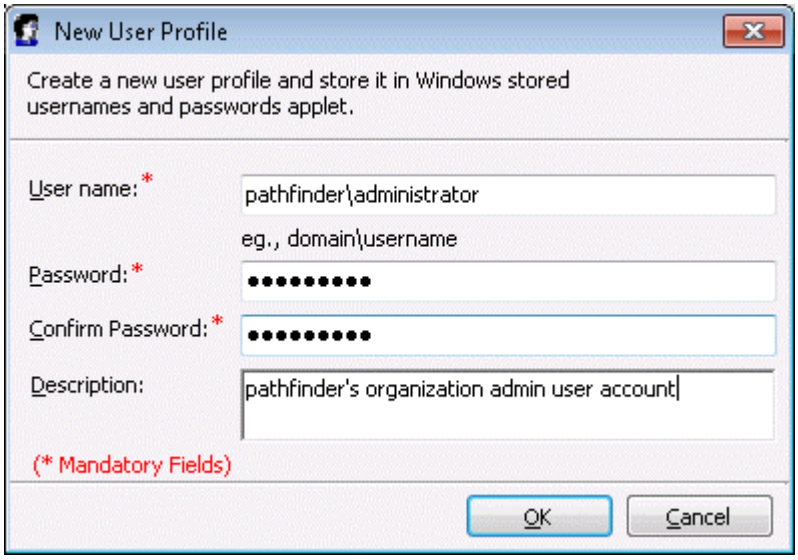
The stored user profile created by ARKAD is restricted to the Windows User Profile context. If the Windows User Profile is maintained locally, ARKAD stored user profile is accessible only by the same user in the same computer. If the user, who creates ARKAD stored user profile, has a *Roaming user account* in the enterprise, the ARKAD stored user profile can be accessed by the same user in any computer in the Windows enterprise.

The stored user profile is a generic credential of **Windows Stored User Names and Passwords** applet and can be used by ARKAD application only. The credential information is stored securely in a 256 *bit encrypted format* in **Windows Stored User Names and Passwords** applet.

Using the **Profile Manager** Dialog shown below, new profile can be **created** and available profiles can be **removed** from the *profiles list.*



Click Add button to add a *new profile* and a dialog will appear as shown below:

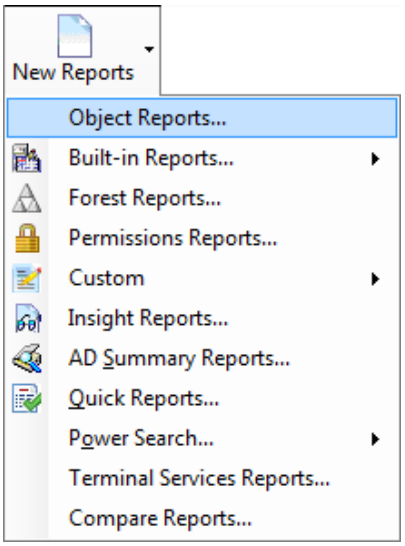


Click Remove button as shown in the *Profile Manager* dialog, to **remove** available profiles.

Chapter 3

3 Object Reports (Working with Reports)

3.1 How to view Domain Reports?



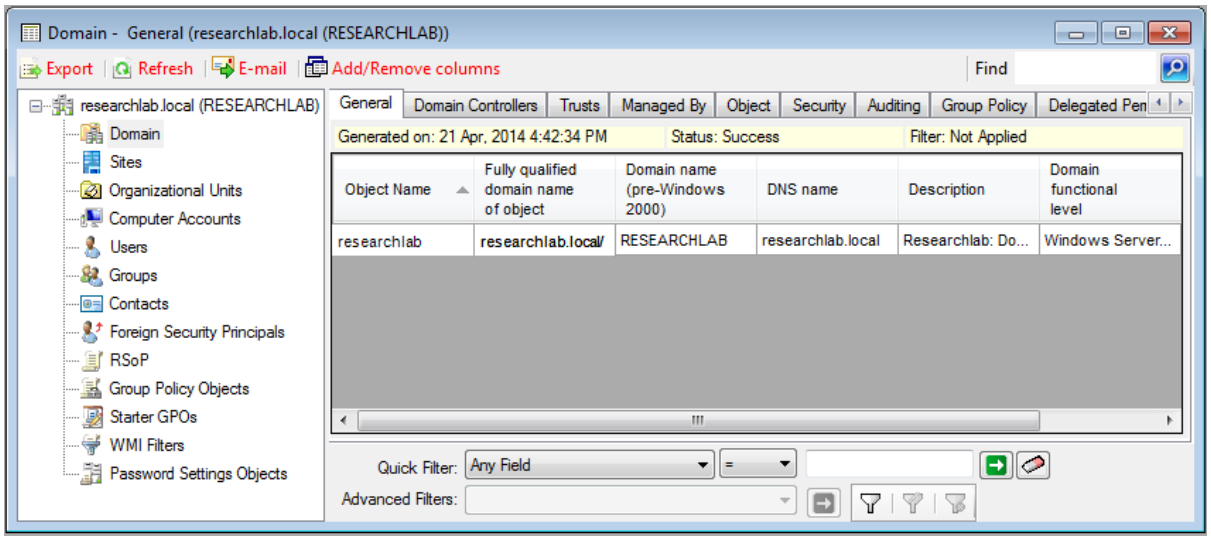
Select option under *New Report* button. The *Connection Manager* will appear on the screen, which will allow you to *select* a *domain* and a corresponding *domain controller*. The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click on **Domain**.

Domain report

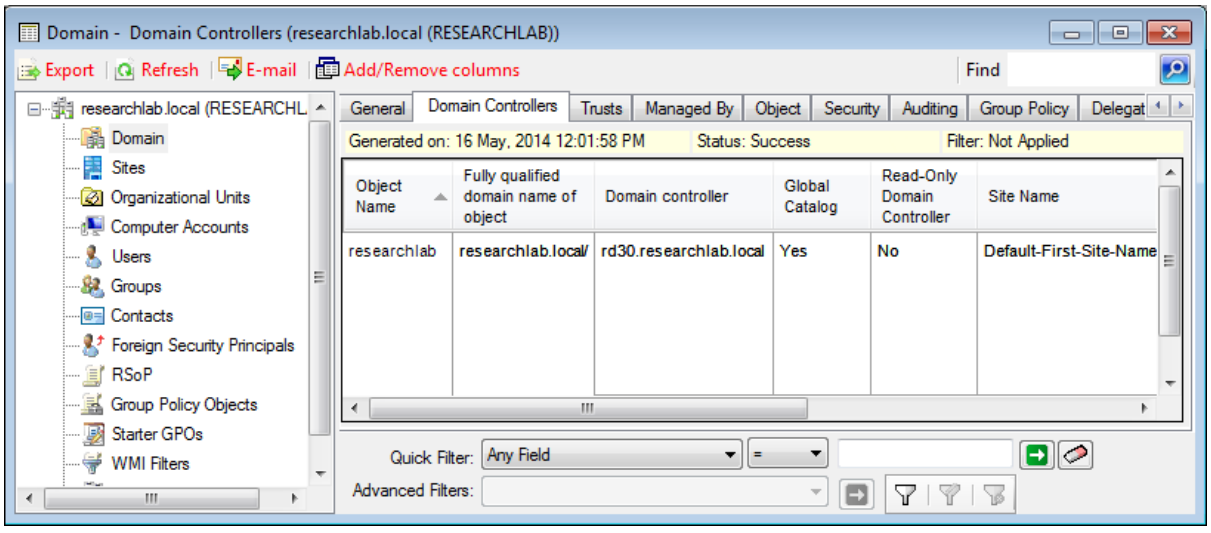
Click on General tab to view the following information:**{Object Name, Fully qualified domain name of object, Domain name (pre-Windows 2000), DNS name, Description, Domain functional level, Forest functional level}.**

The output would be displayed as shown below:



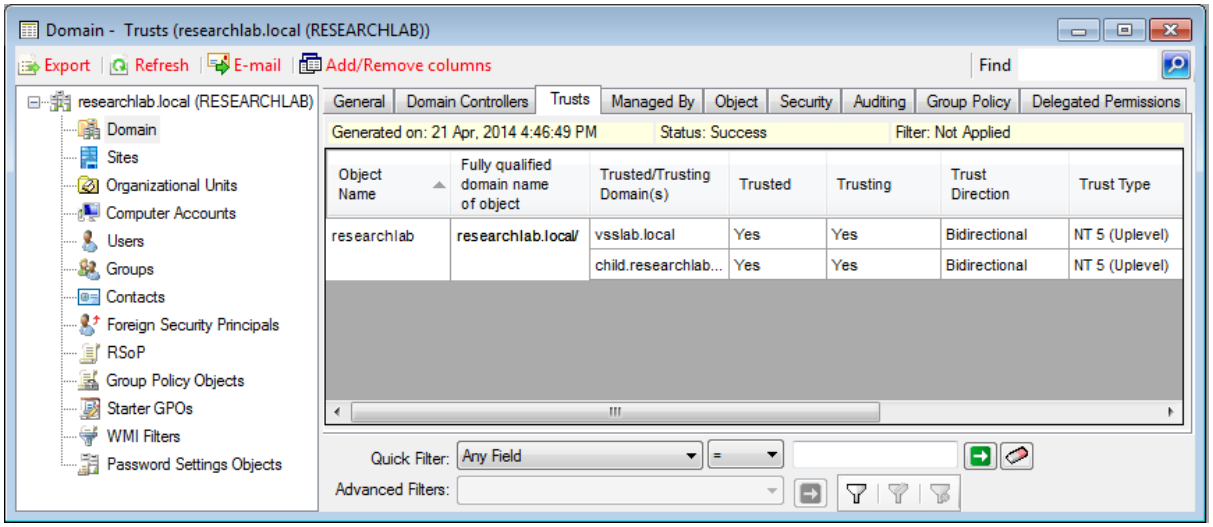
Click on Domain Controllers tab to view the following information:**{Object Name, Fully qualified domain name of object, Domain controller, Global Catalog, Read-Only Domain Controllers (Win 2008), Site Name, Operating System, Service Pack, FSMO role(s), IP Address}.**

The output would be displayed as shown below:



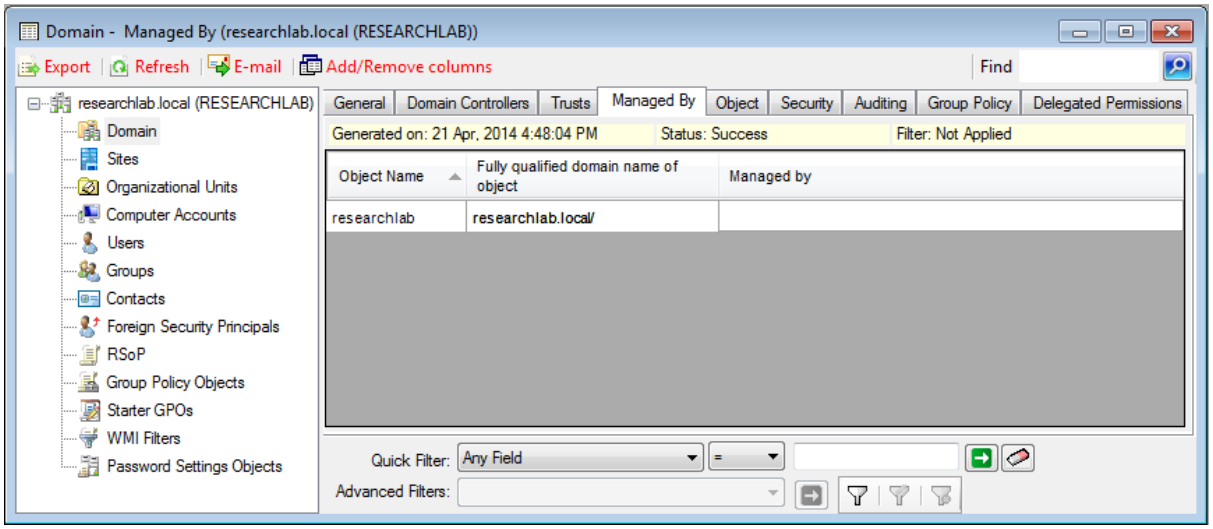
Click on Trusts tab to view the following information:**{Object Name, Fully qualified domain name of object, Trusted/Trusting Domain (s), Trusted, Trusting, Trust Direction, Trust Type, Trust Attributes, Created, and Modified}.**

The output would be displayed as shown below:

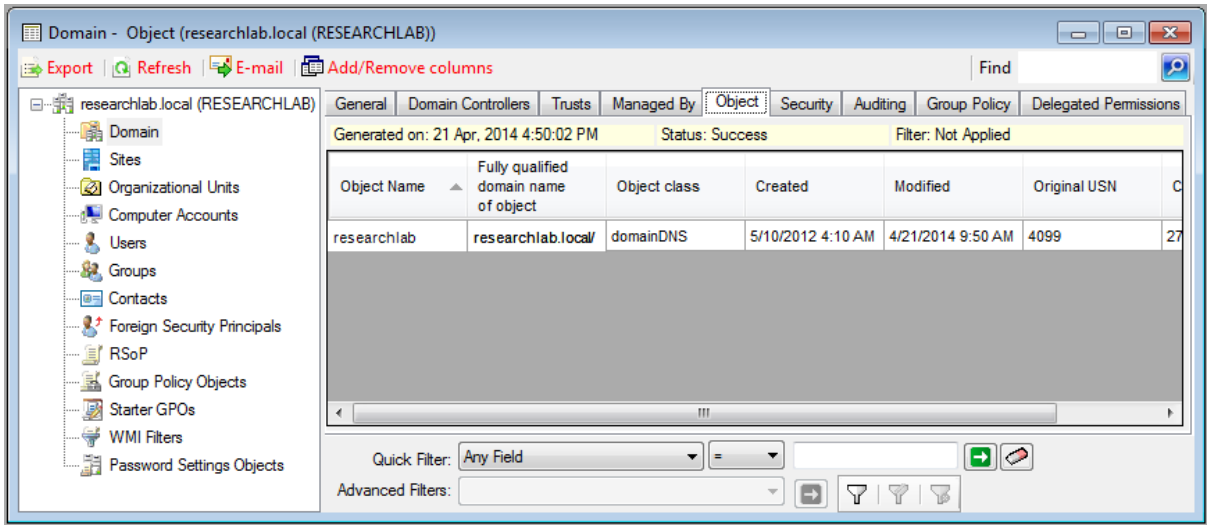


Click on Managed By tab to view the following information :**{ Object Name, Fully qualified domain name of object, Managed By}.**

The output would be displayed as shown below:

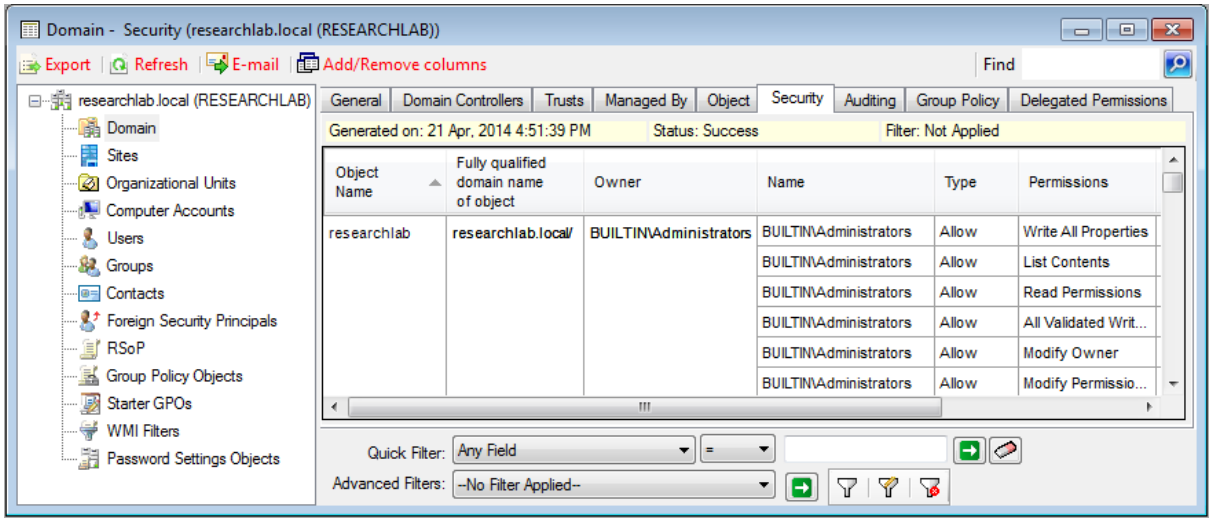


Click on Object tab to view the following information: **{Object Name, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN**The output would be displayed as shown below:



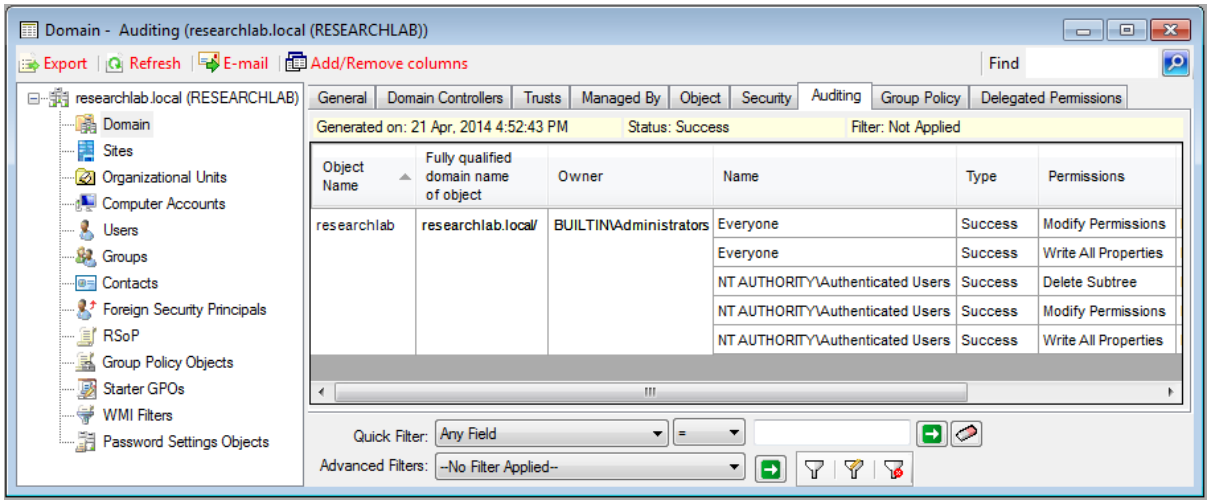
Click on Security tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



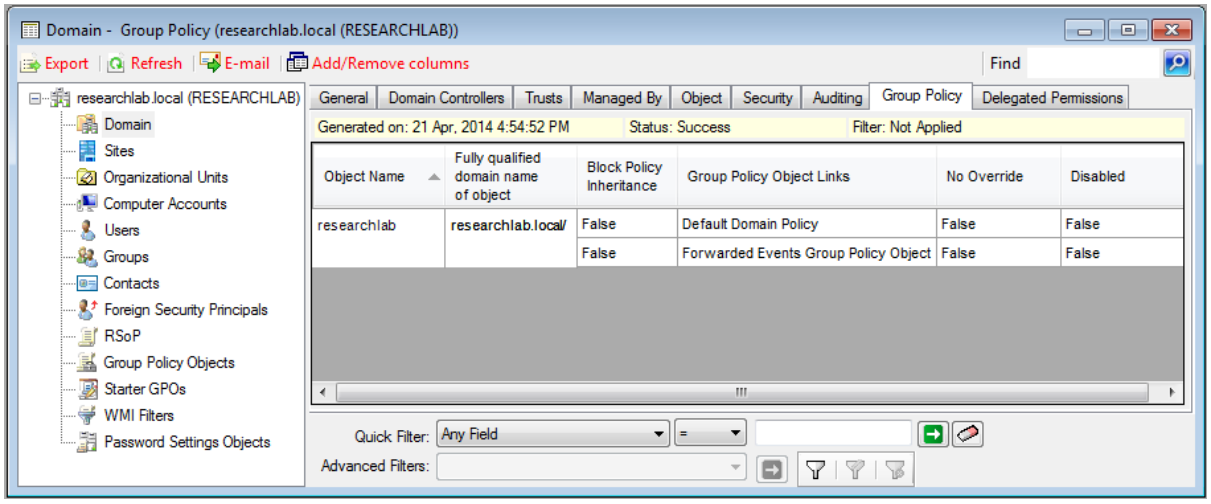
Click on Auditing tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



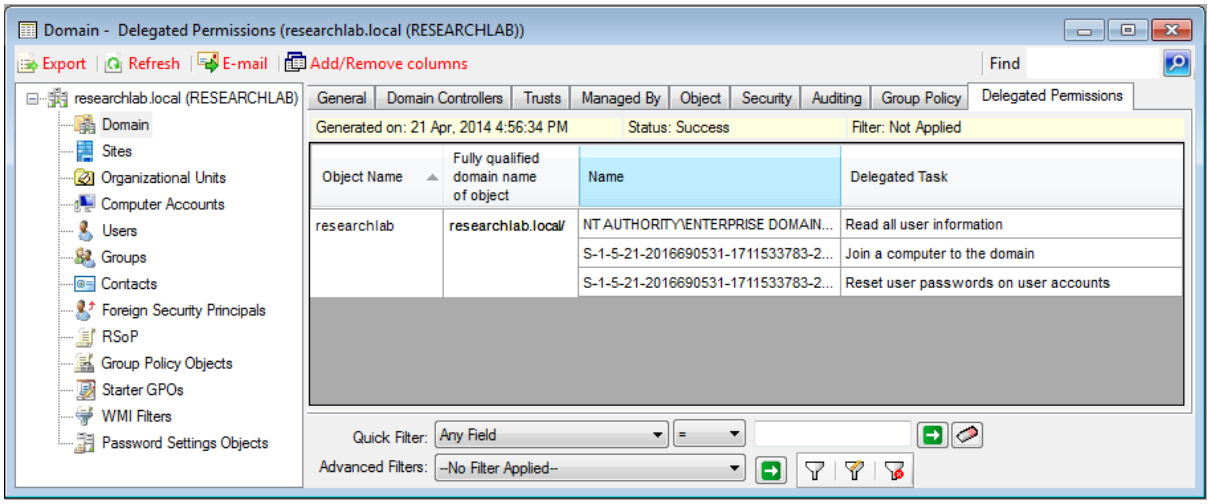
Click on Group Policy tab to view the following information: **{Object Name, Fully qualified domain name of object, Block Policy Inheritance, Group Policy Object Links, No Override, and Disabled}.**

The output would be displayed as shown below:

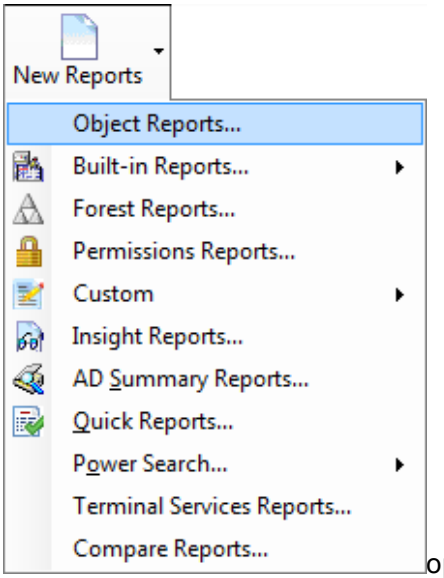


Click on Delegated Permissions Tab to view the following information: {Object Name, Fully qualified domain name of object, Name, Delegated Task

The output would be displayed as shown below:


Domain - Delegated Permissions (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Add/Remove columns
Find
researchlab.local (RESEARCHLAB)
Domain
Sites
Organizational Units
Computer Accounts
Users
Groups
Contacts
Foreign Security Principals
RSoP
Group Policy Objects
Starter GPOs
WMI Filters
Password Settings Objects
General
Domain Controllers
Trusts
Managed By
Object
Security
Auditing
Group Policy
Delegated Permissions
Generated on: 21 Apr, 2014 4:56:34 PM
Status: Success
Filter: Not Applied
Object Name
Fully qualified domain name of object
Name
Delegated Task
researchlab
researchlab.local/
NT AUTHORITY\ENTERPRISE DOMAIN...
Read all user information
S-1-5-21-2016690531-1711533783-2...
Join a computer to the domain
S-1-5-21-2016690531-1711533783-2...
Reset user passwords on user accounts
Quick Filter:
Any Field
=
Advanced Filters:
--No Filter Applied--

3.2 How to view Sites Reports?



Select option under ***New Report*** button. The *Connection Manager w*ill appear on the screen which will allow you to select a *domain* and a corresponding *domain controller*. The report window will be launched after the domain and the selected domain controller are validated.

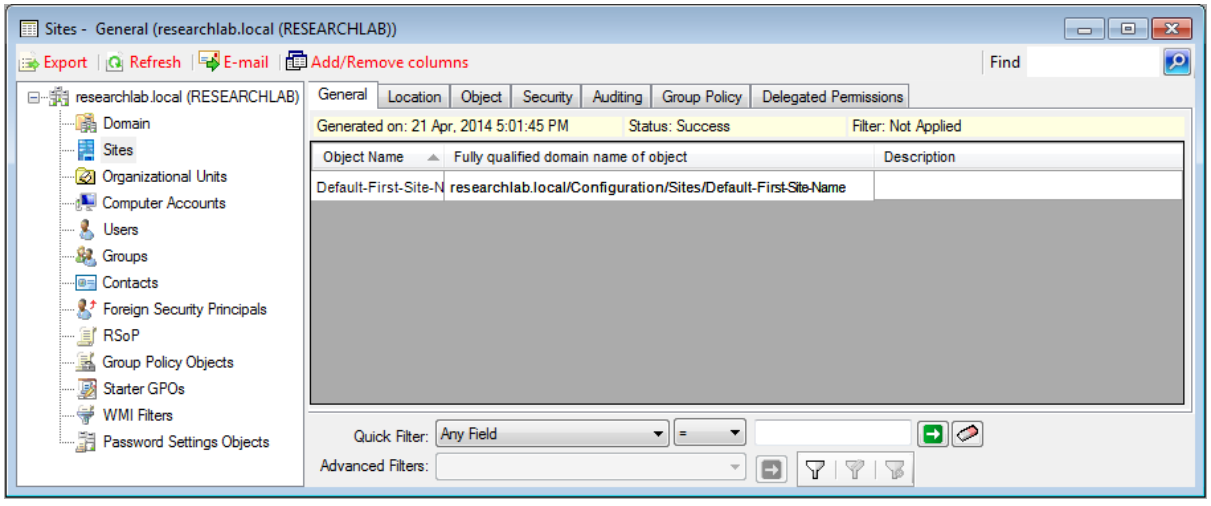
Select and expand the domain node in the left pane of the newly launched report window, and then click on **Sites.**

Sites report

Click on

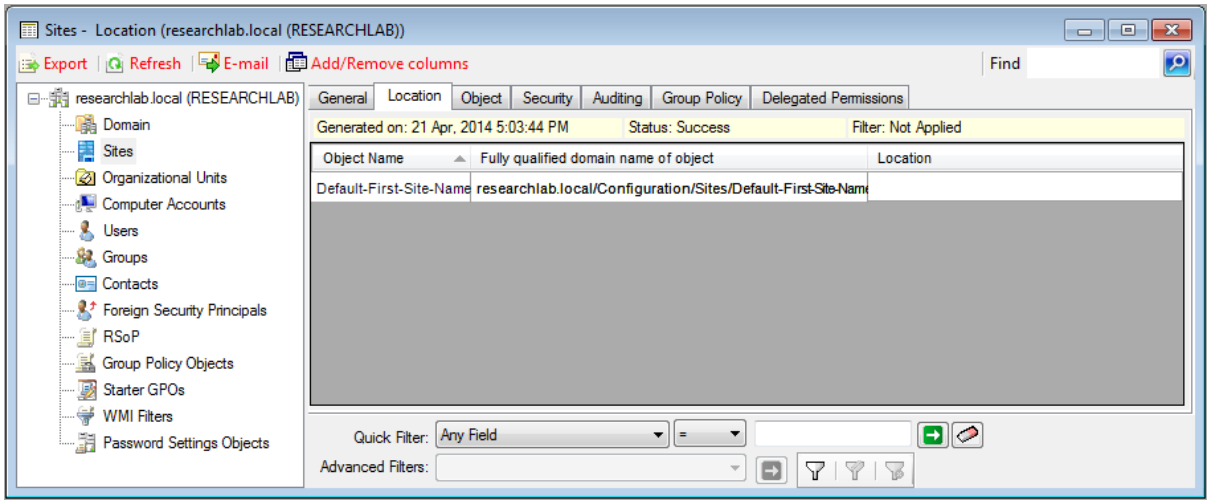
tab to view the following information: **{Object Name, Fully qualified domain name of object, Description}.**

The output would be displayed as shown below:



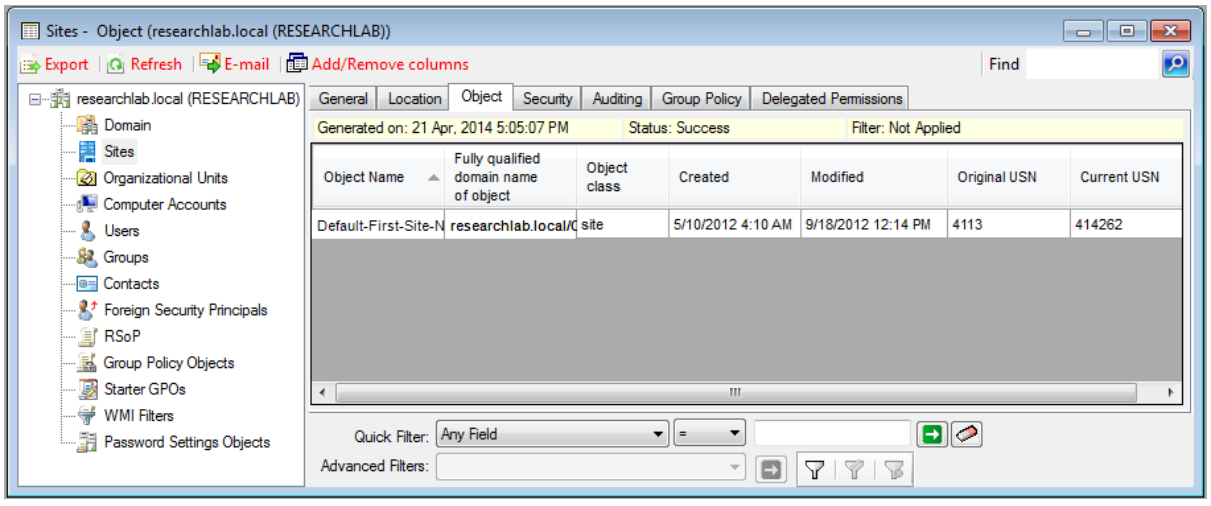
Click on Location tab to view the following information: **{Object Name, Fully qualified domain name of object, Location}.**

The output would be displayed as shown below:



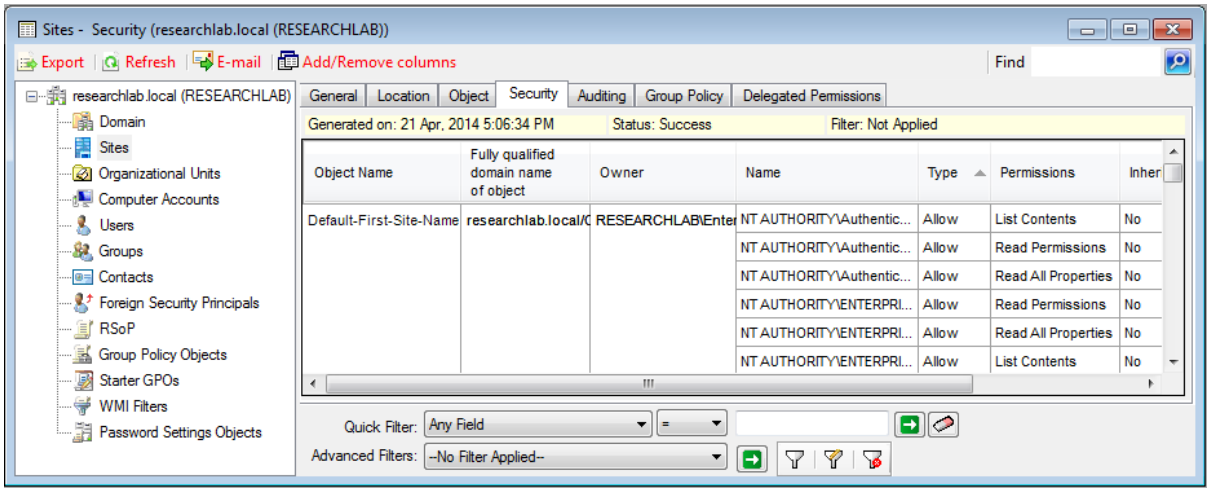
Click on Object tab to view the following information: **{Object Name, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN**

The output would be displayed as shown below:



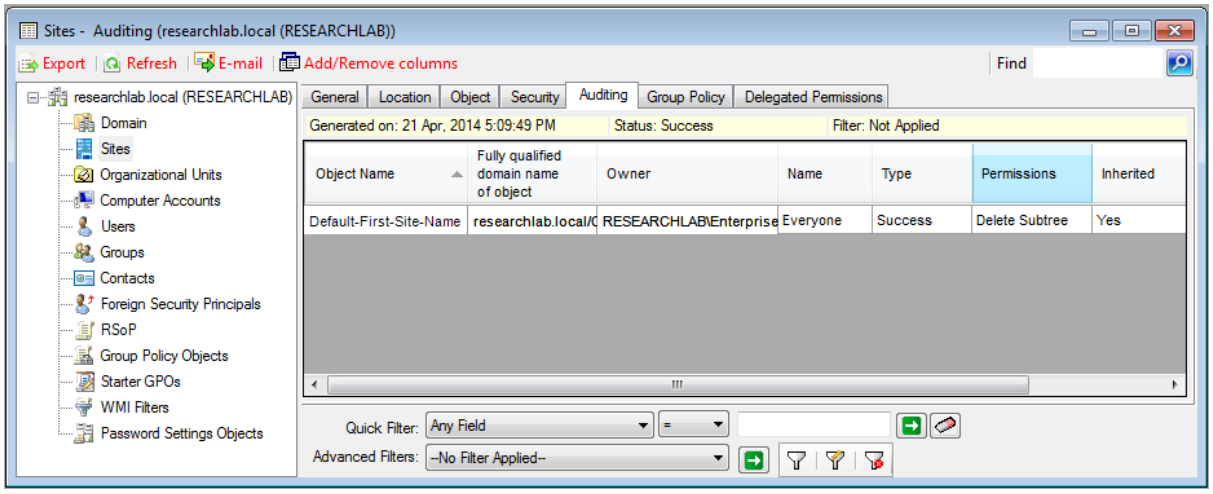
Click on Security tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:

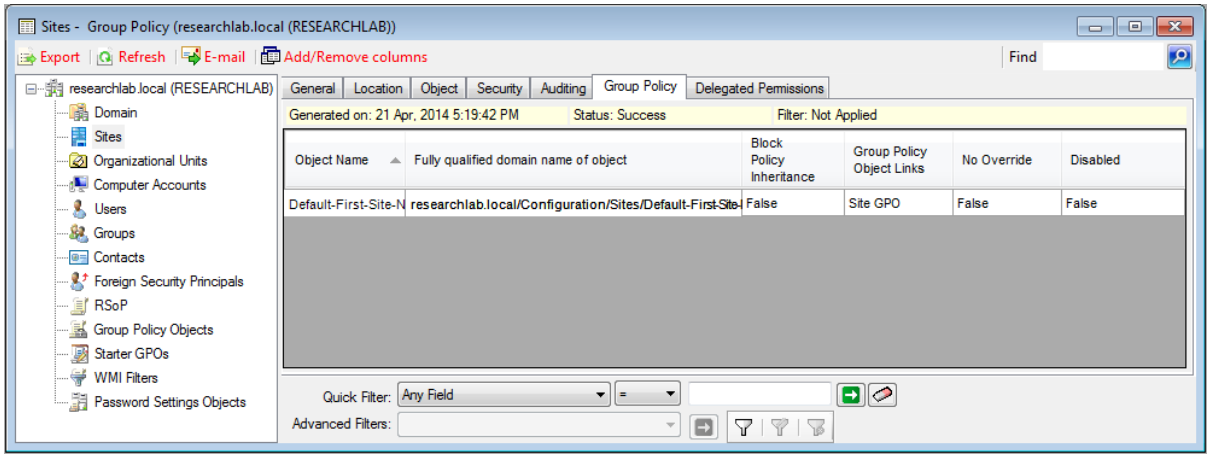


Click on Auditing tab to *view* the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:

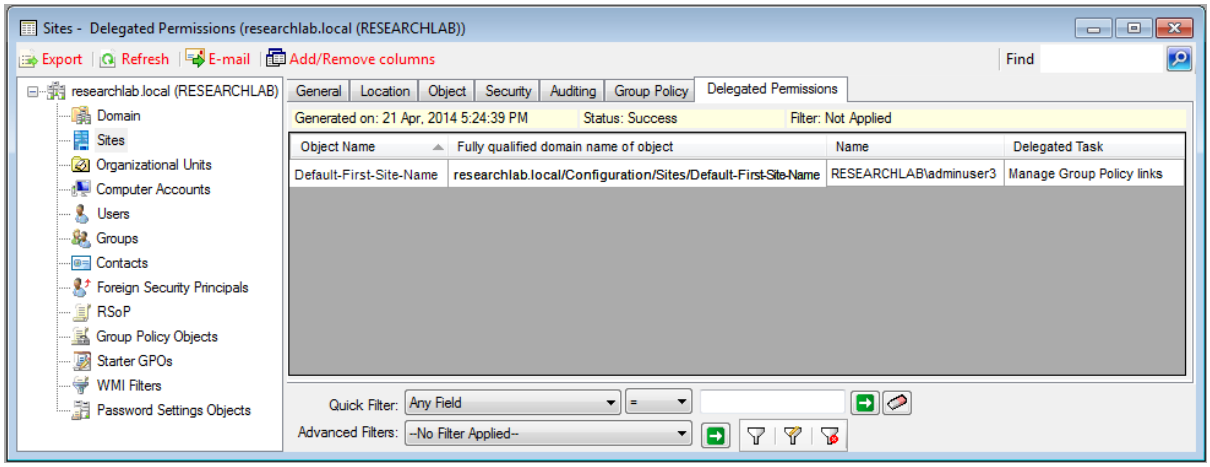


Click on Group Policy tab to *view* the following information: **{Object Name, Fully qualified domain name of object, Block Policy Inheritance, Group Policy Object Links, No Override, and Disabled}.**

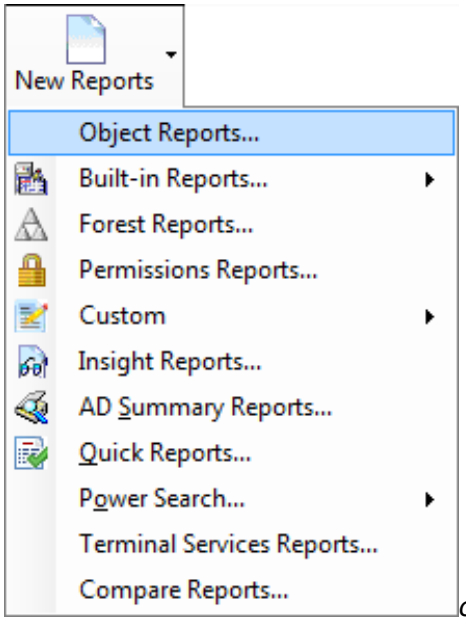


Click on tab to view the following information: **{Object Name, Fully qualified domain name of object, Name, Delegated Task}.**

The output would be displayed as shown below:



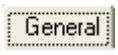
3.3 How to view Organizational Unit Reports



Select *option* under ***New Report*** button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

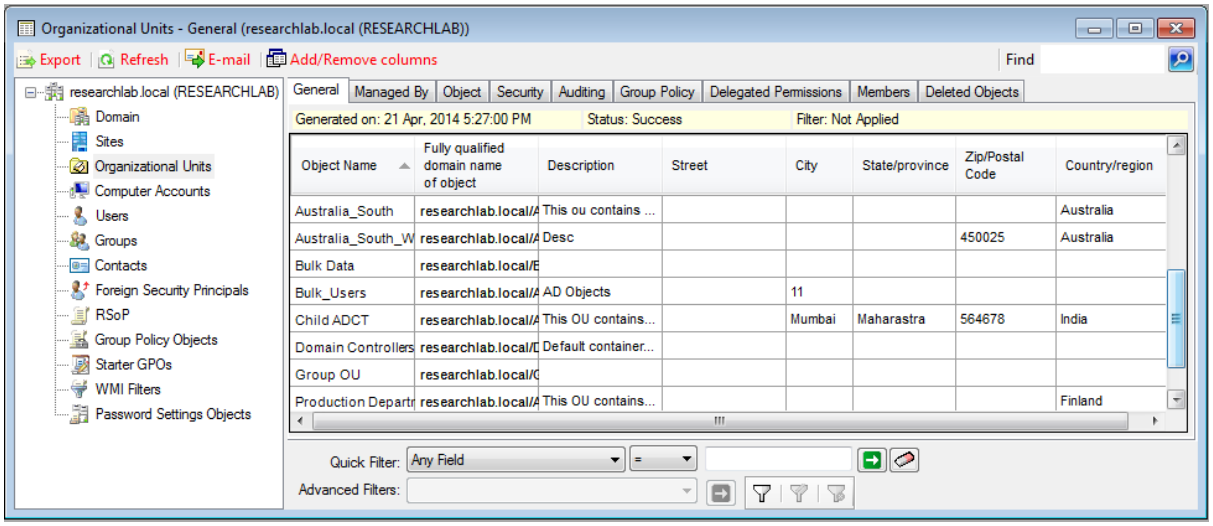
Select and expand the domain node in the left pane of the newly launched report window, and then click on **Organizational Units.**

Organizational Unit General Report

Click on 

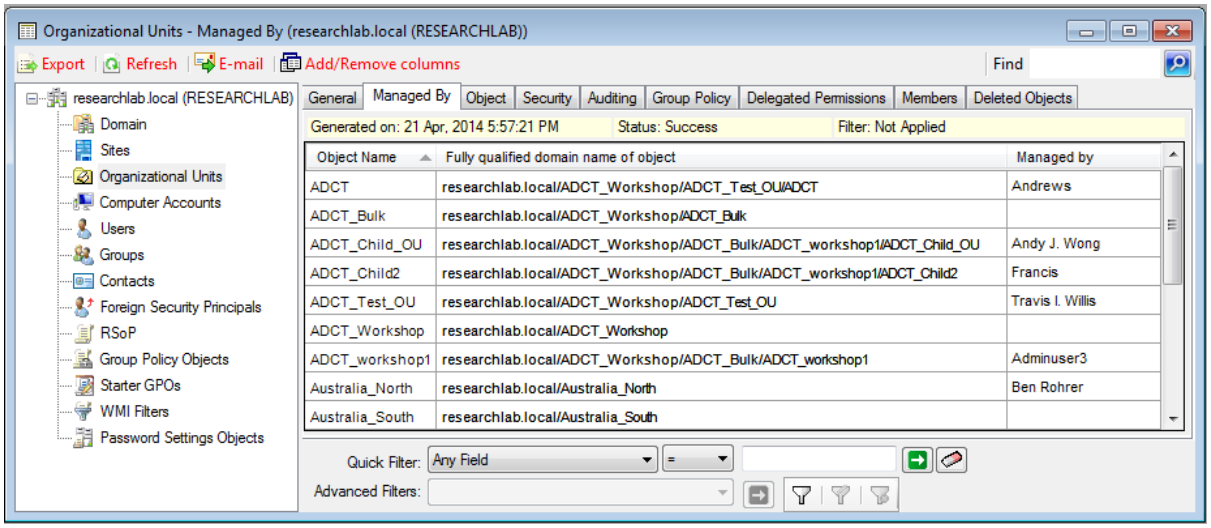
tab to view the following information: **{Object Name, Fully qualified domain name of object, Description, Street, City, State/province, Zip/Postal Code, and Country/region}.**

The output would be displayed as shown below:



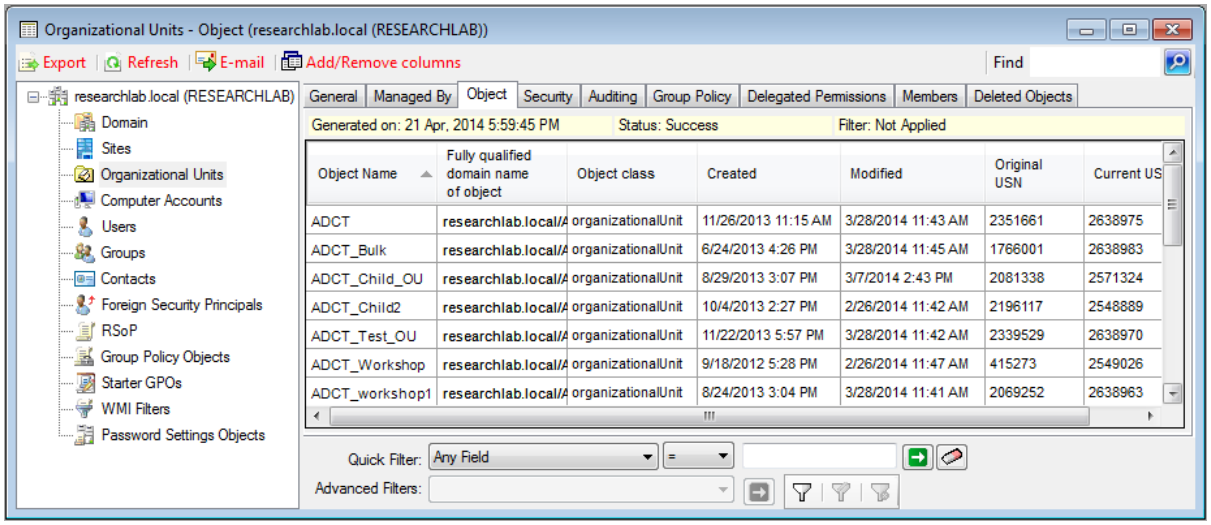
Click on Managed By tab to view the following information: **{Object Name, Fully qualified domain name of object, Managed By}.**

The output would be displayed as shown below:



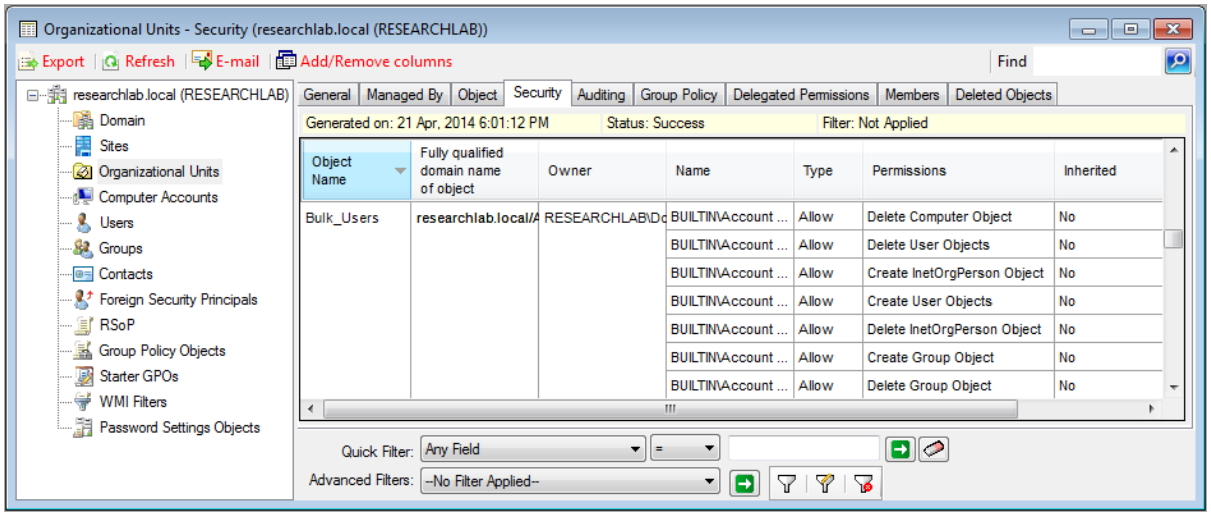
Click on Object tab to view the following information: **{Object Name, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN}.**

The output would be displayed as shown below:



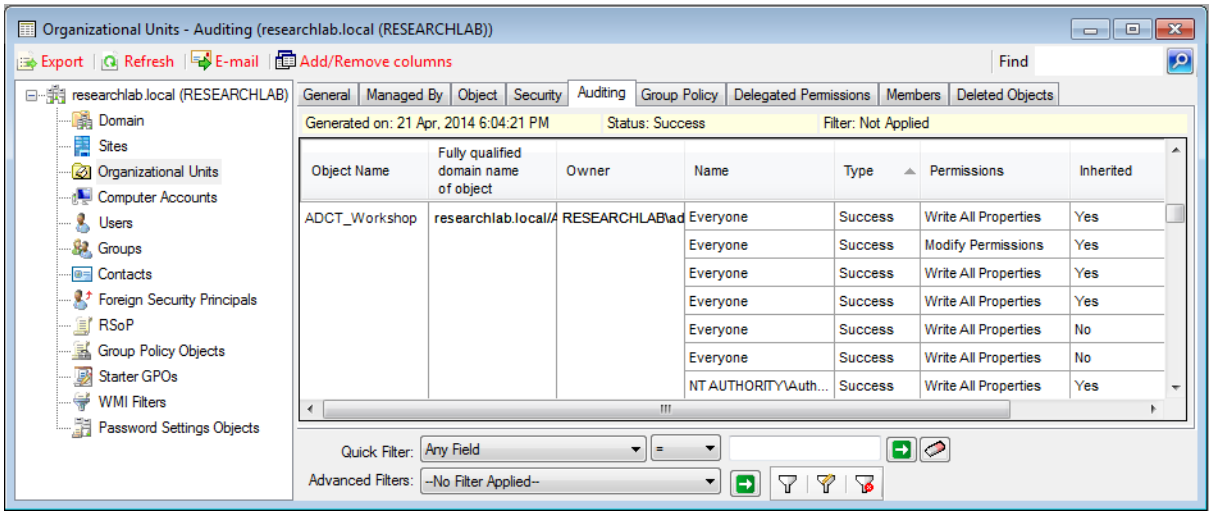
Click on Security tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



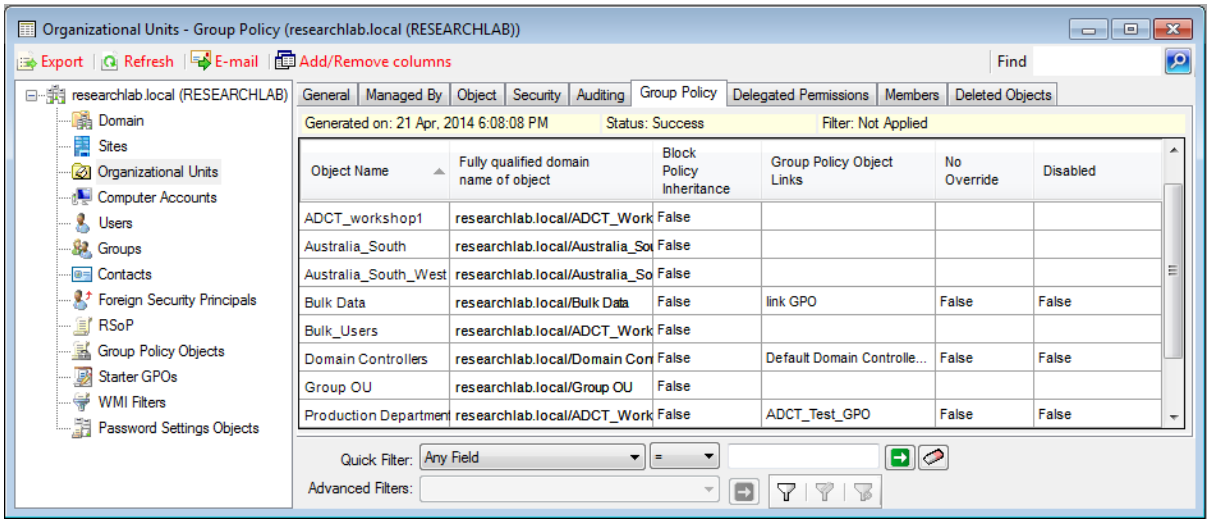
Click on Auditing tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



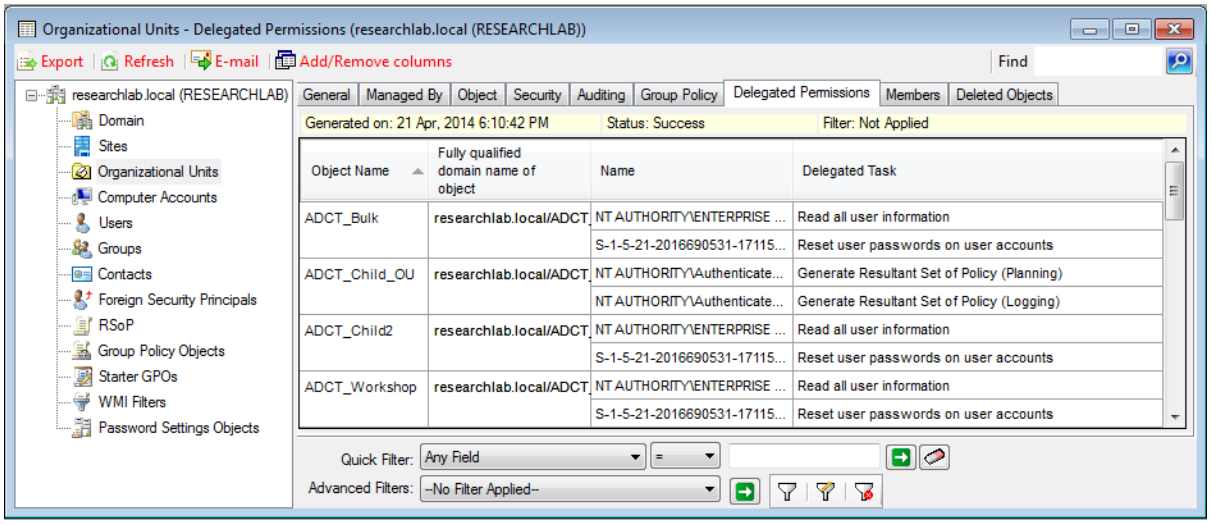
Click on Group Policy tab to view the following information: **{Object Name, Fully qualified domain name of object, Block Policy Inheritance, Group Policy Object Links, No Override, and Disabled}.**

The output would be displayed as shown below:



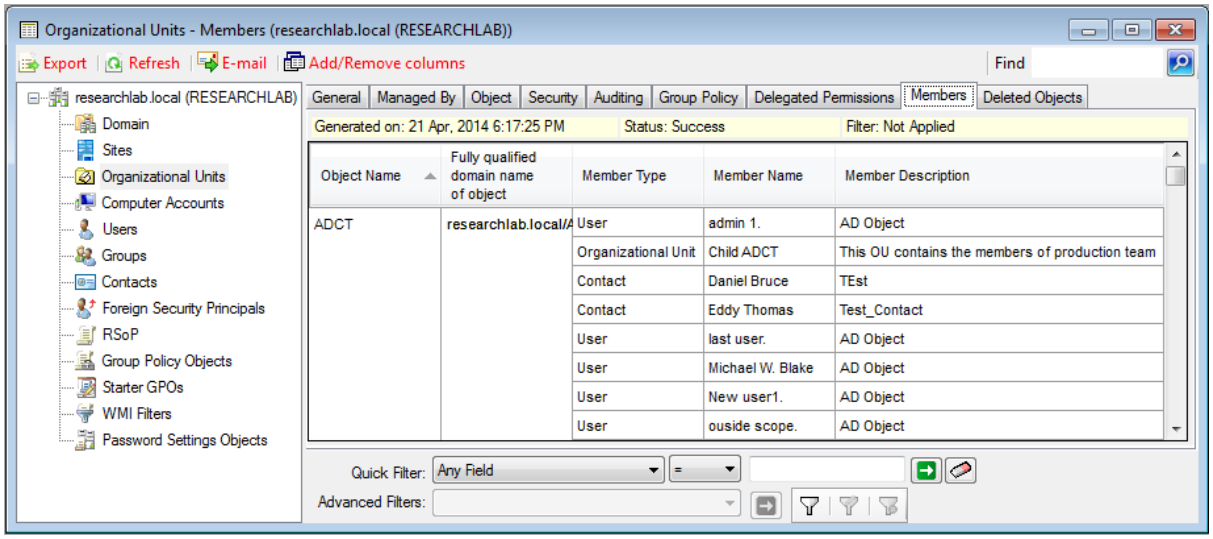
Click on Delegated Permissions tab to view the following information: **{Object Name, Fully qualified domain name of object, Name, Delegated Task}.**

The output would be displayed as shown below:



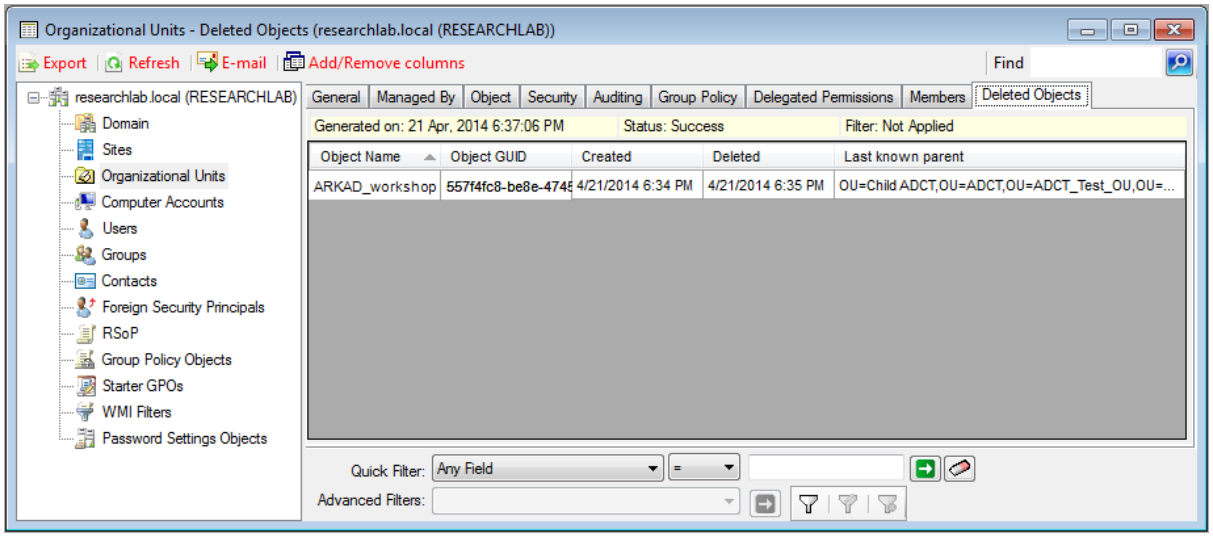
Click on tab to view the following information: **{Object Name, Fully qualified domain name of object, Member Type, Member Name}.**

The output would be displayed as shown below:



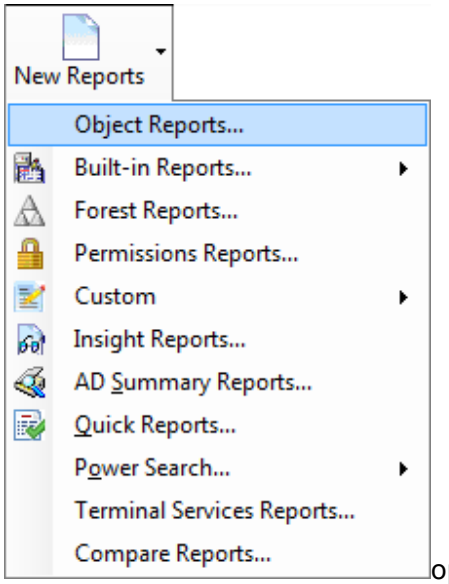
Click on tab to view the following information: **{Object Name, Object GUID, Created, Deleted, Last known parent}.**

The output would be displayed as shown below:



NOTE: The *"Last known parent"* attribute would be set only on a Windows Server 2003 domain controller and later.

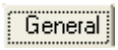
3.4 How to view Computer Accounts Reports?



Select option under ***New Report*** button. The *Connection Manager* will appear on the screen, which will allow you to *select* a *domain* and a corresponding *domain controller*. The report window will be launched after the domain and the selected domain controller are validated.

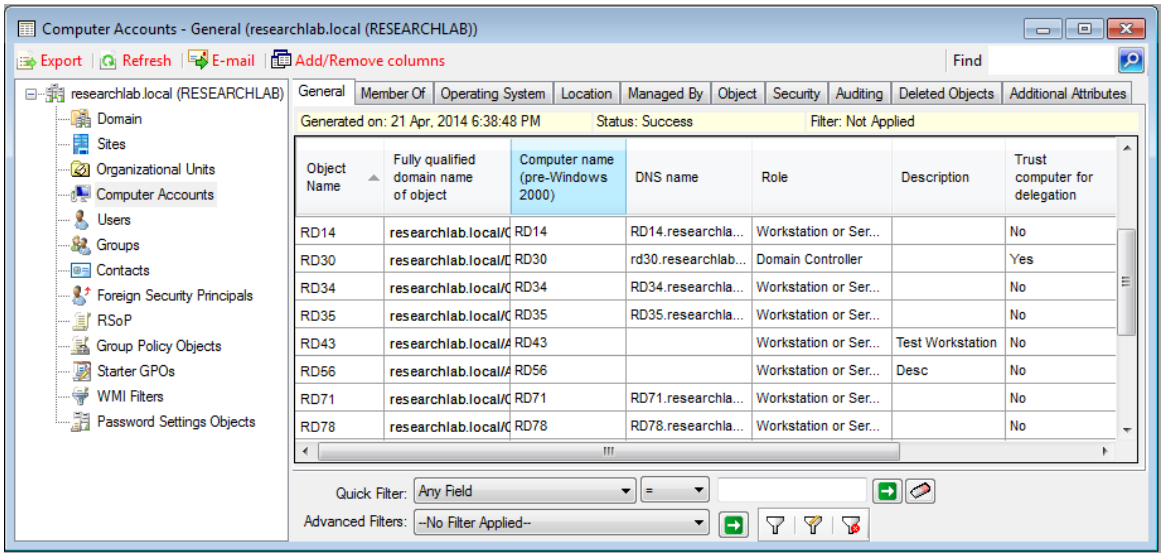
Select and expand the domain node in the left pane in the newly launched report window, and then click on **Computer Accounts.**

Computer Accounts Reports

Click on 

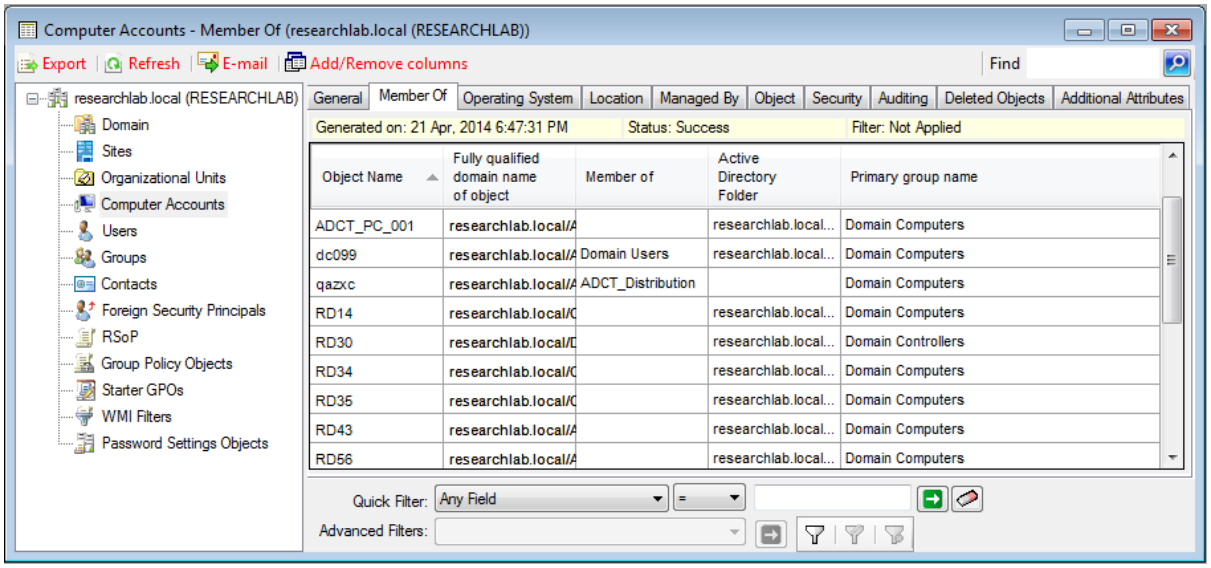
tab to view the following information: **{Object Name, Fully qualified domain name of object, Computer name (pre-Windows 2000), DNS name, Role, Description, Trust computer for delegation, Account is disabled, Last Logon}.**

The output would be displayed as shown below:



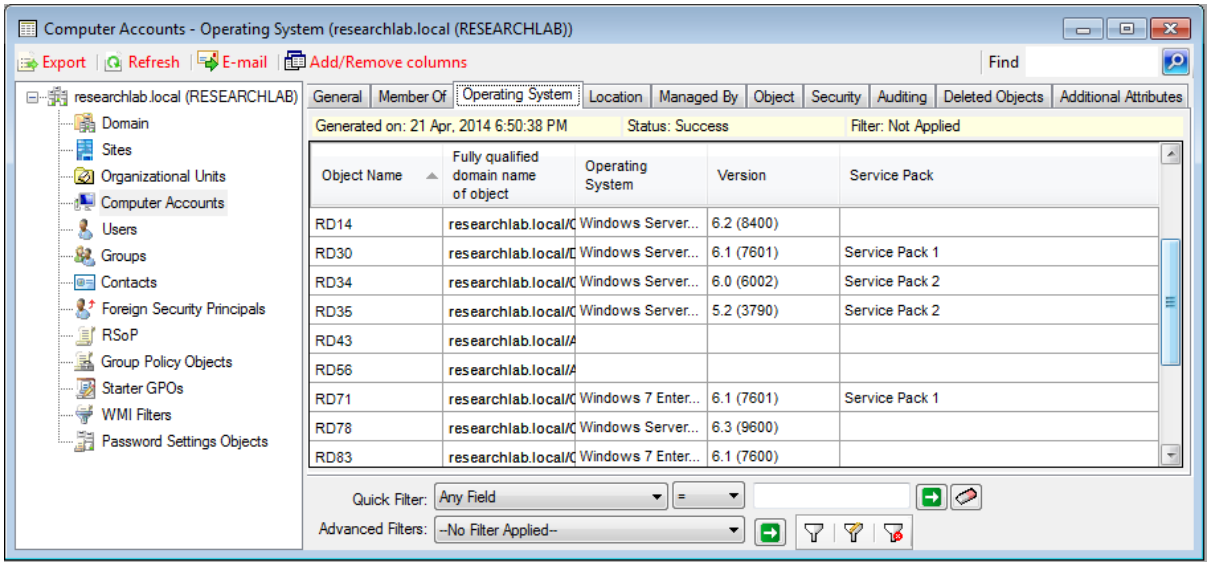
Click on Member Of tab to view the following information: **{Object Name, Fully qualified domain name of object, Member of, Active Directory Folder, Primary group name}.**

The output would be displayed as shown below:



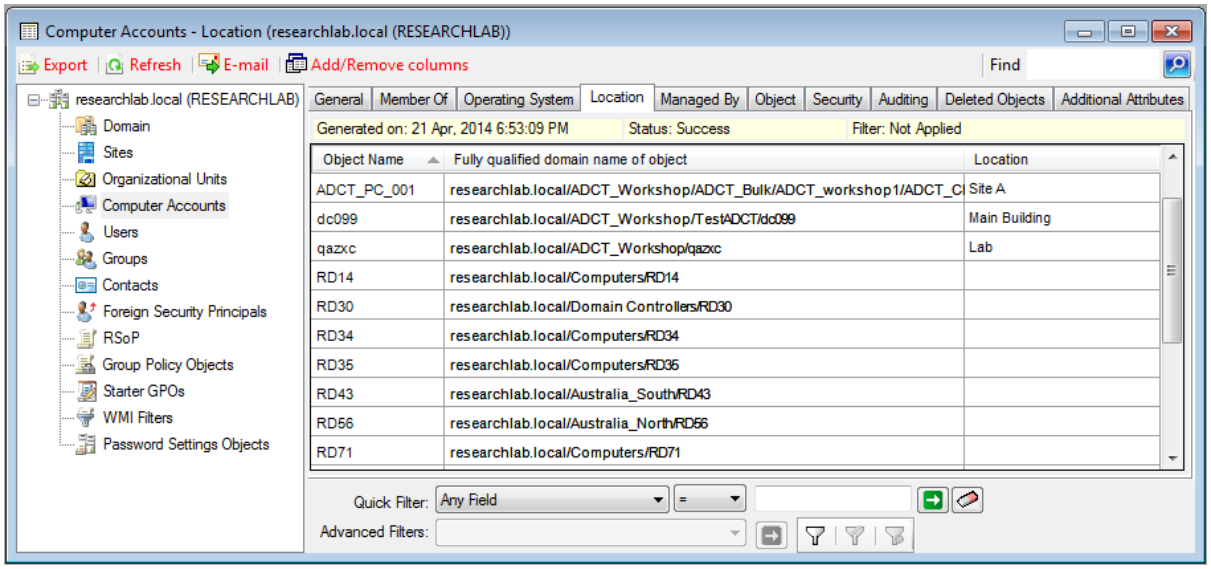
Click on Operating System tab to view the following information: **{Object Name, Fully qualified domain name of object, Operating System, Version, Service Pack}.**

The output would be displayed as shown below:



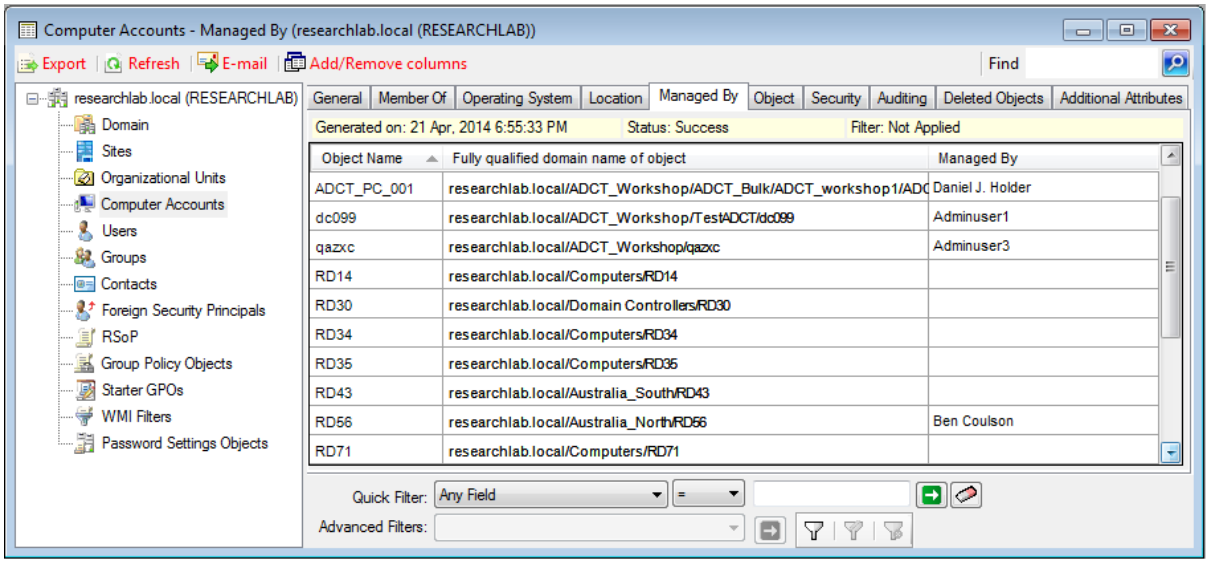
Click on Location tab to view the following information: **{Object Name, Fully qualified domain name of object, Location}.**

The output would be displayed as shown below:



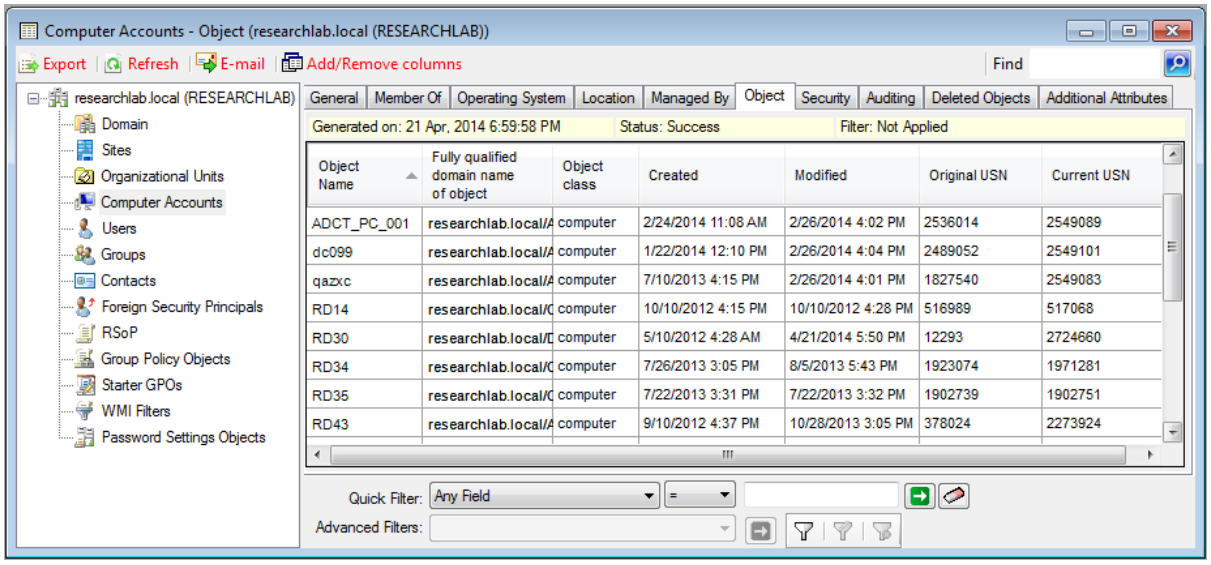
Click on Managed By tab to view the following information: **{Object Name, Fully qualified domain name of object, Managed By}.**

The output would be displayed as shown below:



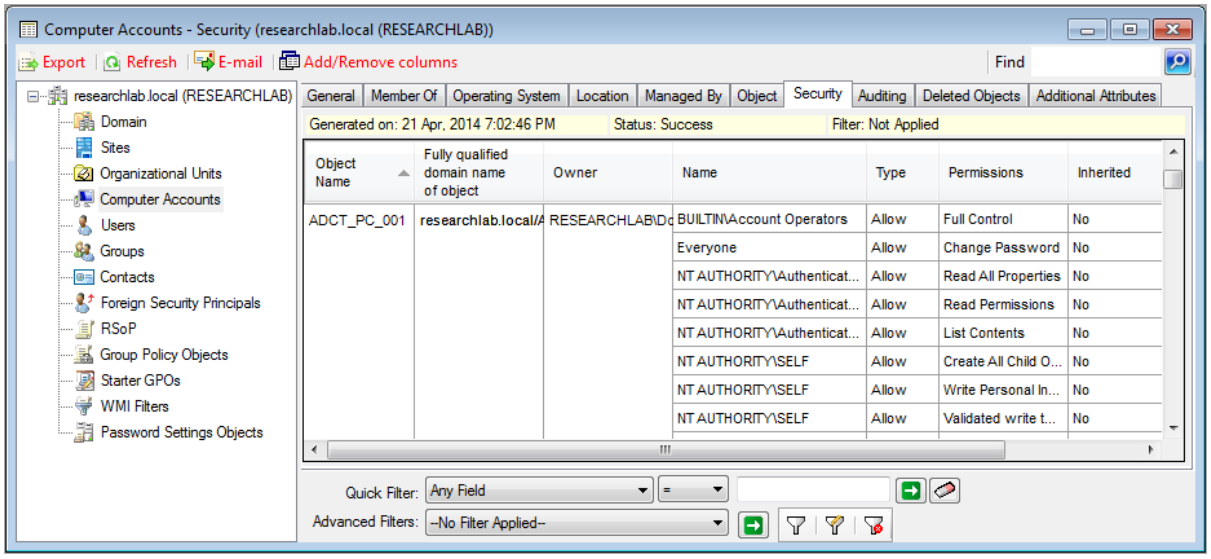
Click on Object tab to view the following information: **{Object Name, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN}.**

The output would be displayed as shown below:



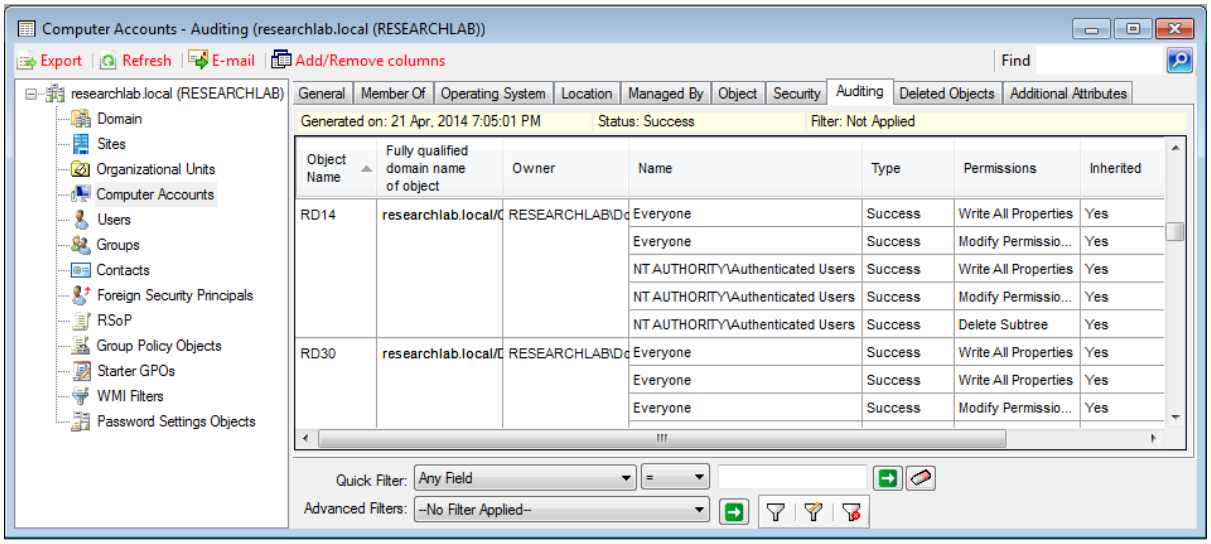
Click on Security tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



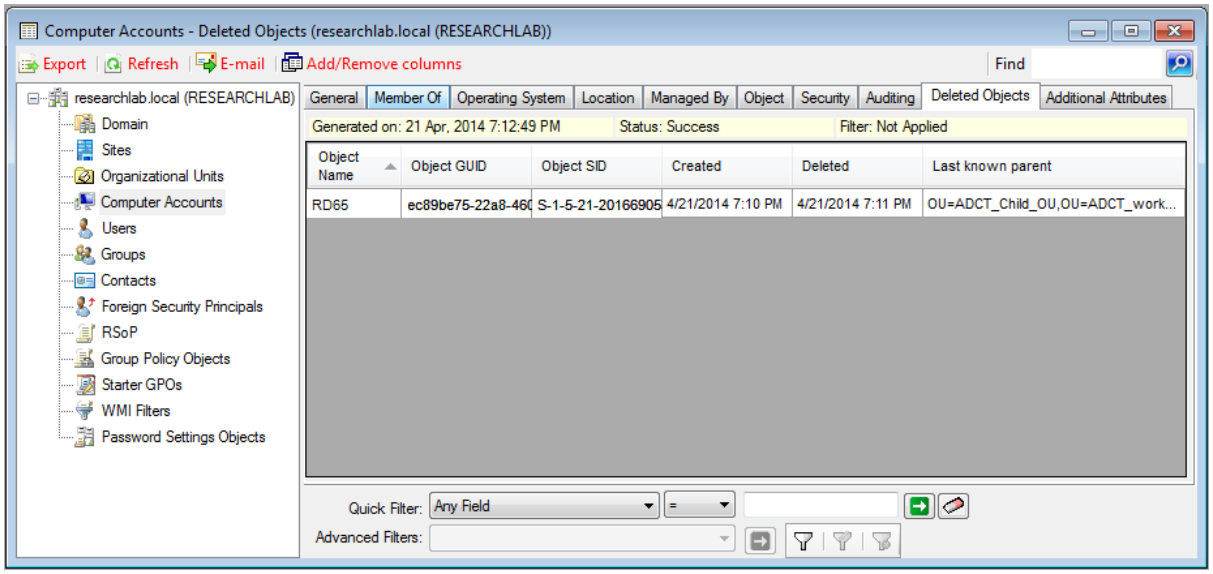
Click on Auditing tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



Click on Deleted Objects tab to view the following information: **{Object Name, Object GUID, Object SID, Created, Deleted, Last known parent}.**

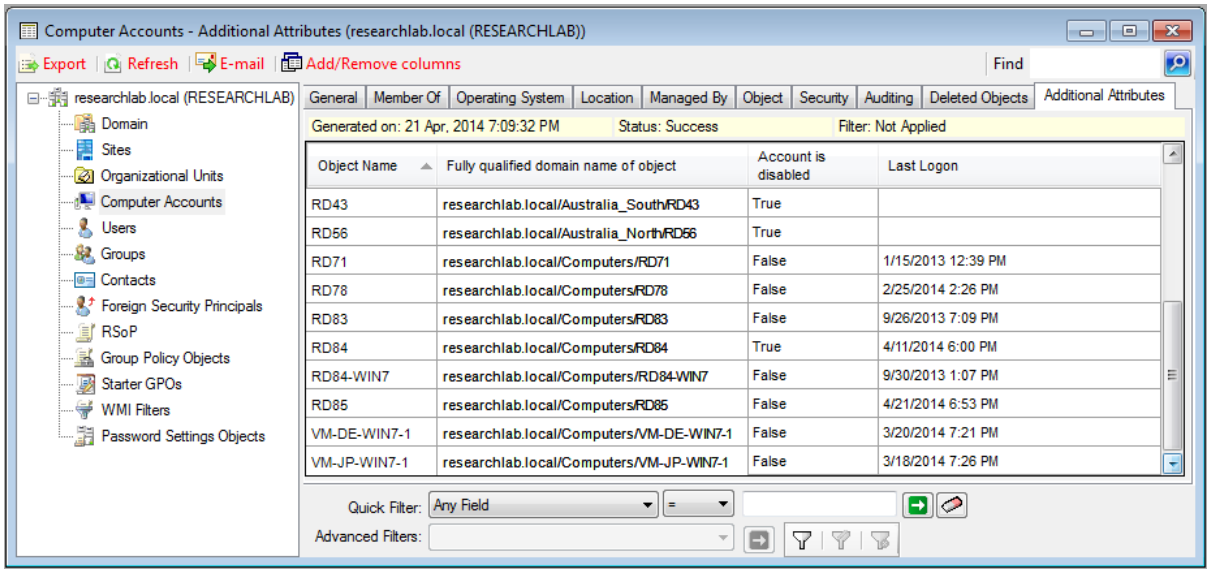
The output would be displayed as shown below:



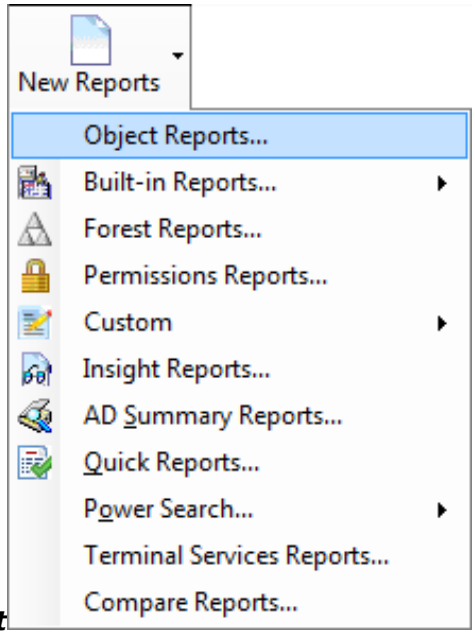
NOTE: The *"Last known parent"* attribute would be set only on a *Windows Server 2003* domain controller and later.

Click on Additional Attributes tab to view the following information: **{Object Name, Fully qualified domain name of object, Account is disabled, Last Logon}.**

The output would be displayed as shown below:


Computer Accounts - Additional Attributes (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Add/Remove columns
Find
researchlab.local (RESEARCHLAB)
Domain
Sites
Organizational Units
Computer Accounts
Users
Groups
Contacts
Foreign Security Principals
RSoP
Group Policy Objects
Starter GPOs
WMI Filters
Password Settings Objects
General
Member Of
Operating System
Location
Managed By
Object
Security
Auditing
Deleted Objects
Additional Attributes
Generated on: 21 Apr, 2014 7:09:32 PM
Status: Success
Filter: Not Applied
Object Name
Fully qualified domain name of object
Account is disabled
Last Logon
RD43 researchlab.local/Australia_South/RD43 True
RD56 researchlab.local/Australia_North/RD56 True
RD71 researchlab.local/Computers/RD71 False 1/15/2013 12:39 PM
RD78 researchlab.local/Computers/RD78 False 2/25/2014 2:26 PM
RD83 researchlab.local/Computers/RD83 False 9/26/2013 7:09 PM
RD84 researchlab.local/Computers/RD84 True 4/11/2014 6:00 PM
RD84-WIN7 researchlab.local/Computers/RD84-WIN7 False 9/30/2013 1:07 PM
RD85 researchlab.local/Computers/RD85 False 4/21/2014 6:53 PM
VM-DE-WIN7-1 researchlab.local/Computers/VM-DE-WIN7-1 False 3/20/2014 7:21 PM
VM-JP-WIN7-1 researchlab.local/Computers/VM-JP-WIN7-1 False 3/18/2014 7:26 PM
Quick Filter:
Any Field
=
Advanced Filters:

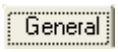
3.5 How to view Users Reports?



Select option under ***New Report*** button. The *Connection Manager* will appear on the screen, which will allow you to *select* a *domain* and a corresponding *domain controller*. The report window will be launched after the domain and the selected domain controller are validated.

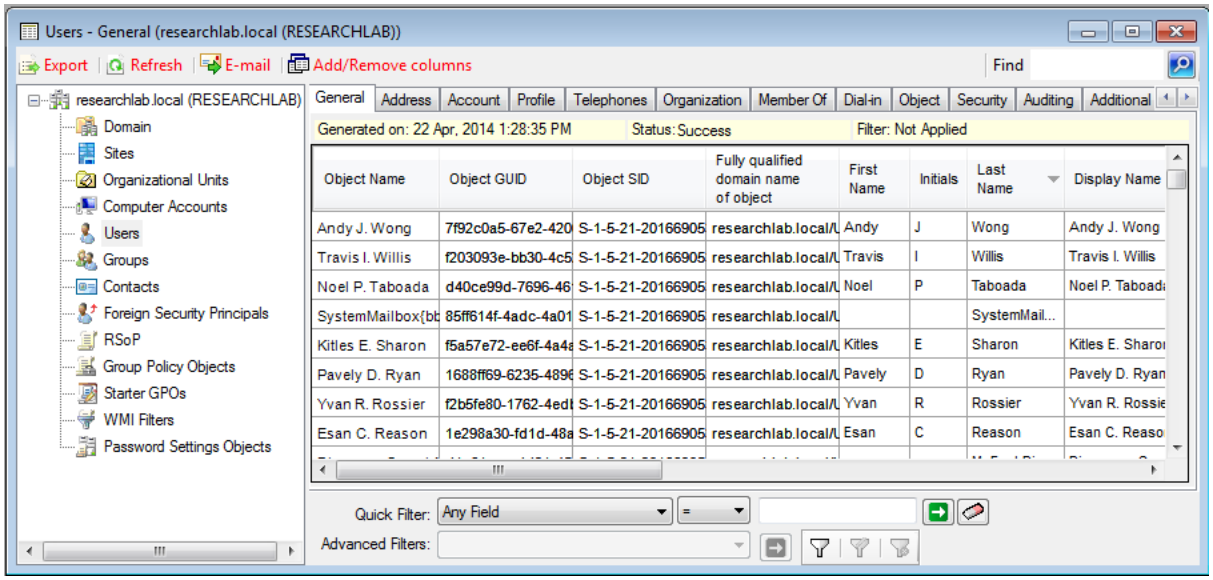
Select and expand the domain node in the left pane of the newly launched report window, and then click on **Users.**

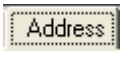
Users report

Click on 

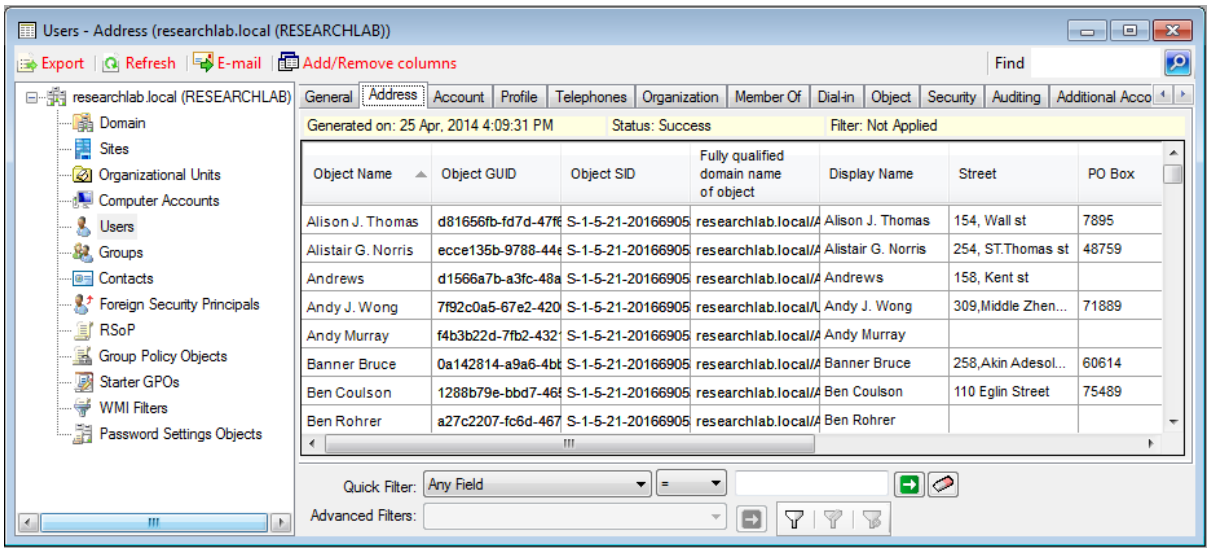
tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, First Name, Initials, Last Name, Display Name, Description, Employee ID, Employee Number, Office, Telephone Number, Phone Numbers (Others), E-mail, Web Page, Web Page Address (Others)}.**

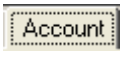
The output would be displayed as shown below:



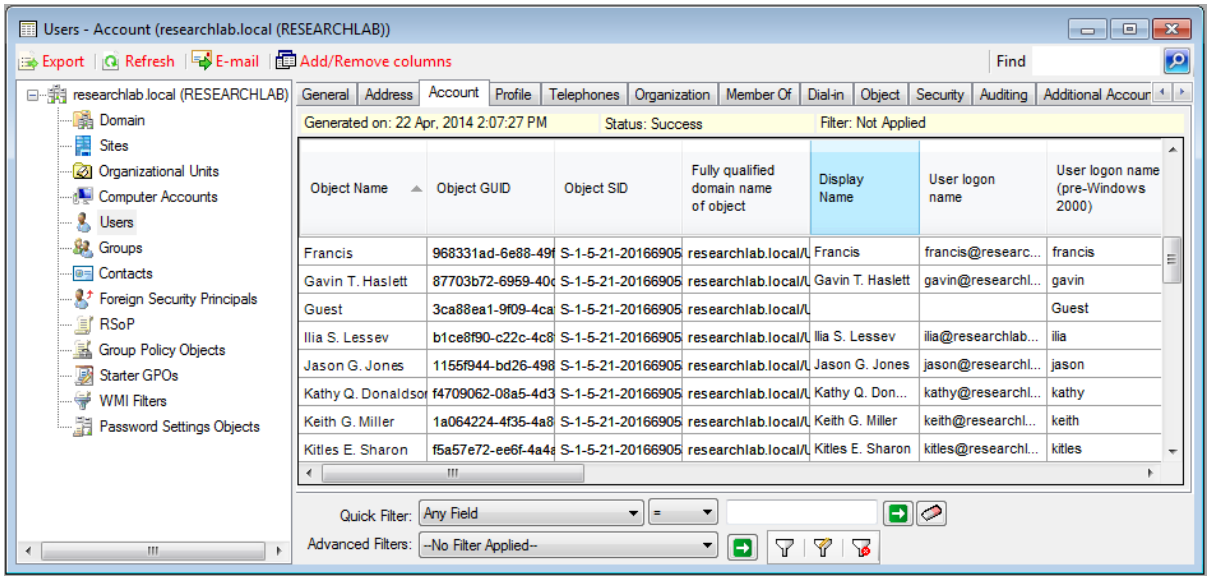
Click on  tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Display Name, Street, PO Box, City, State/Province, Zip/Postal Code, Country/Region}.**

The output would be displayed as shown below:



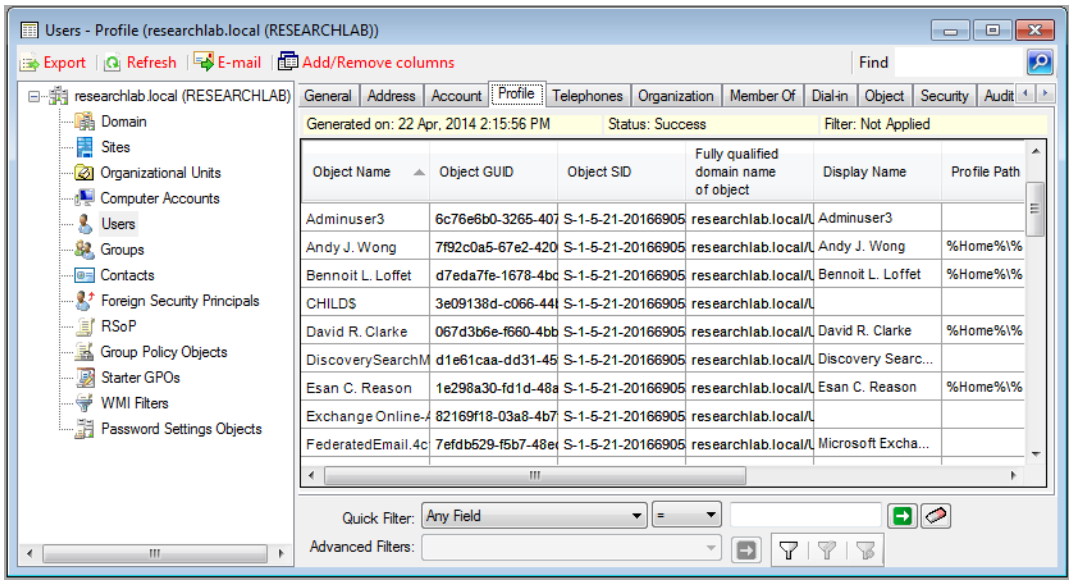
Click on  tab to view the following information: *{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Display Name, User logon name, User logon name (pre-Windows 2000), Log On To, Account is locked out, User must change password at next logon, User cannot change password, Password never expires, Store password using reversible encryption, Account is disabled, Smart card is required for interactive logon, Account is trusted for delegation, Account is sensitive and cannot be delegated, Use DES encryption types for this account, Do not require Kerberos preauthentication, Account expires, Account expiration date}.*

The output would be displayed as shown below:



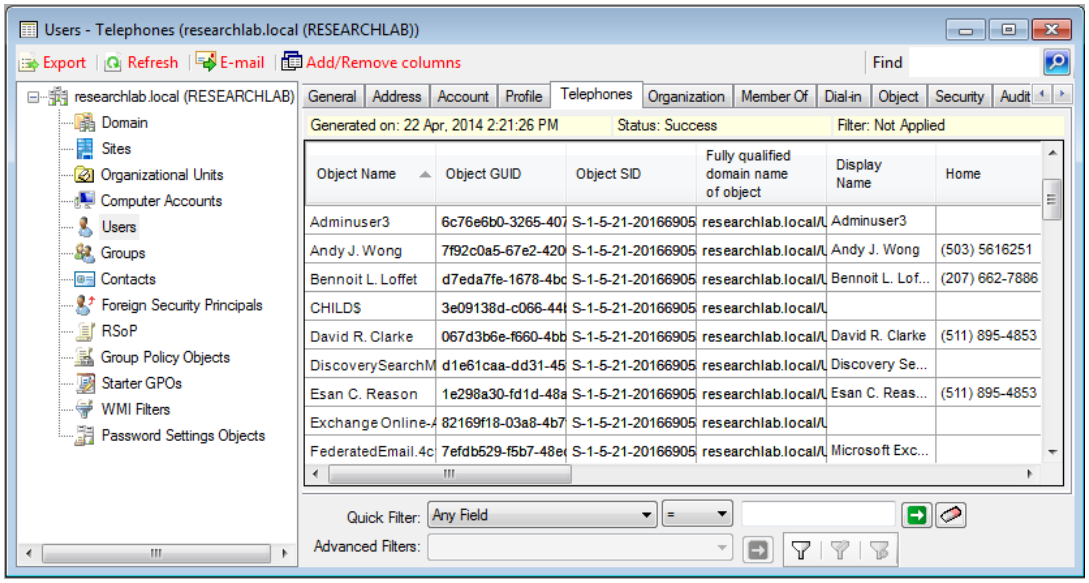
Click on Profile tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Display Name, Profile Path, Logon Script, Local Path, Connect to}.**

The output would be displayed as shown below:



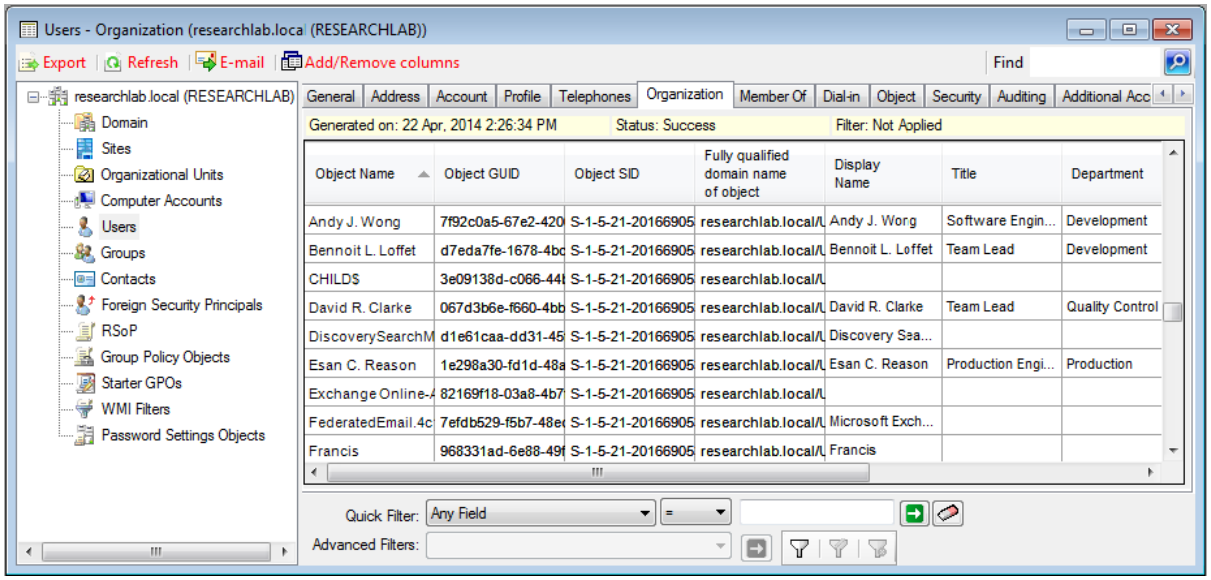
Click Telephones on tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Display Name, Home, Home Phone (Others), Pager, Pager Number (Others), Mobile, Mobile Number (Others), Fax, Fax Number (Others), IP Phone, IP Phone Number (Others), Notes}.**

The output would be displayed as shown below:



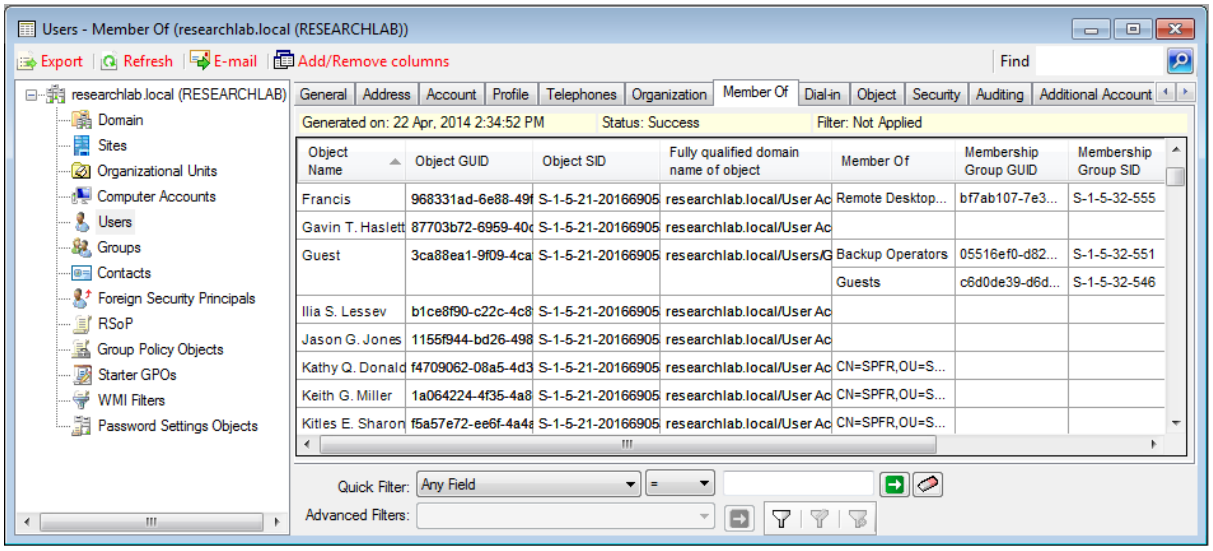
Click on Organization tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Display Name, Title, Department, Company, Manager, Direct Reports}.**

The output would be displayed as shown below:



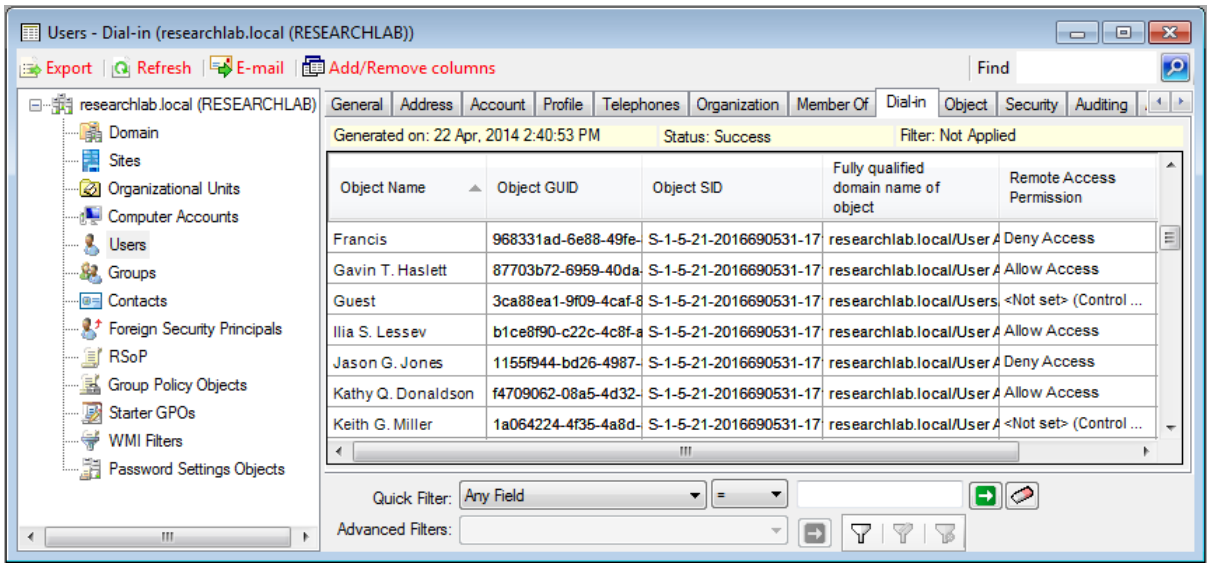
Click Member Of on tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Member Of, Membership Group GUID, Membership Group SID, Membership Group FQDN, Primary group name}.**

The output would be displayed as shown below:



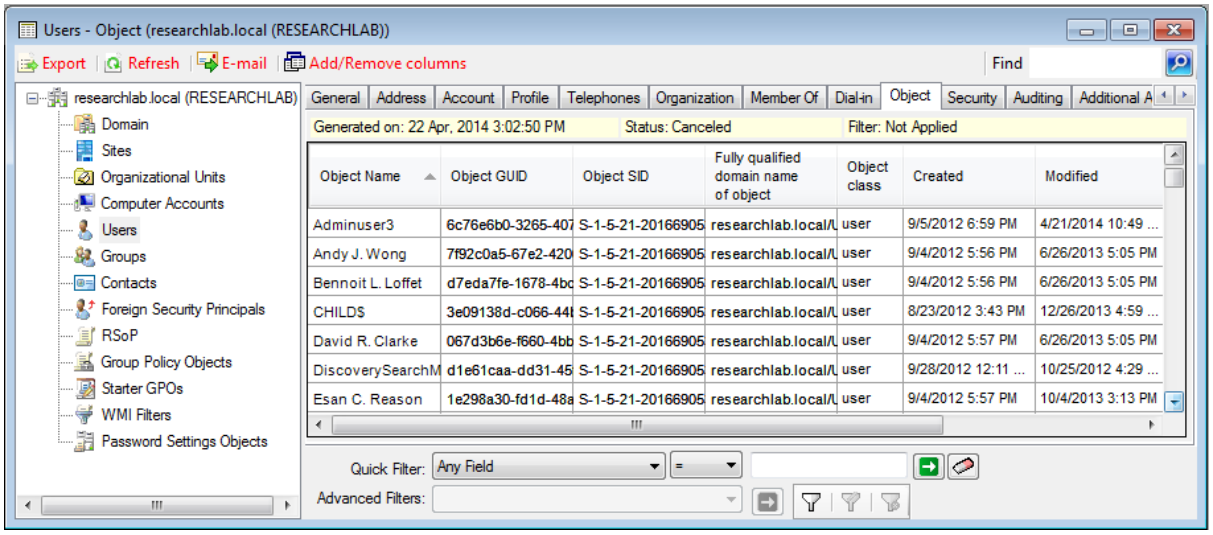
Click on Dial-in tab to view the following information: **{Object Name, Object GUID, Object SID, Object GUID, Object SID, Fully qualified domain name of object, Remote Access Permission, Call-back Option}.**

The output would be displayed as shown below:



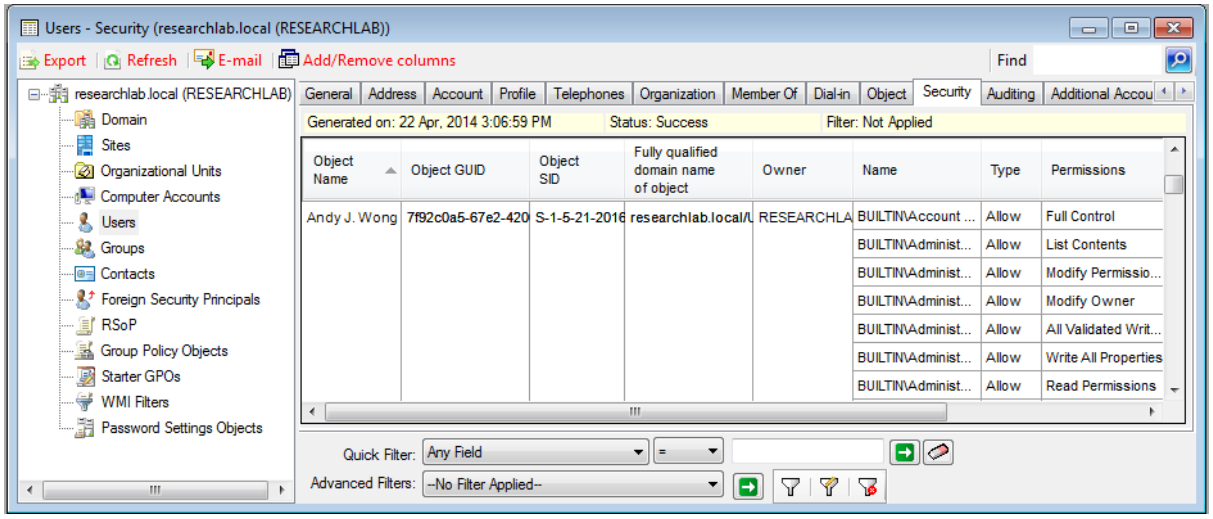
Click on Object tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN}.**

The output would be displayed as shown below:



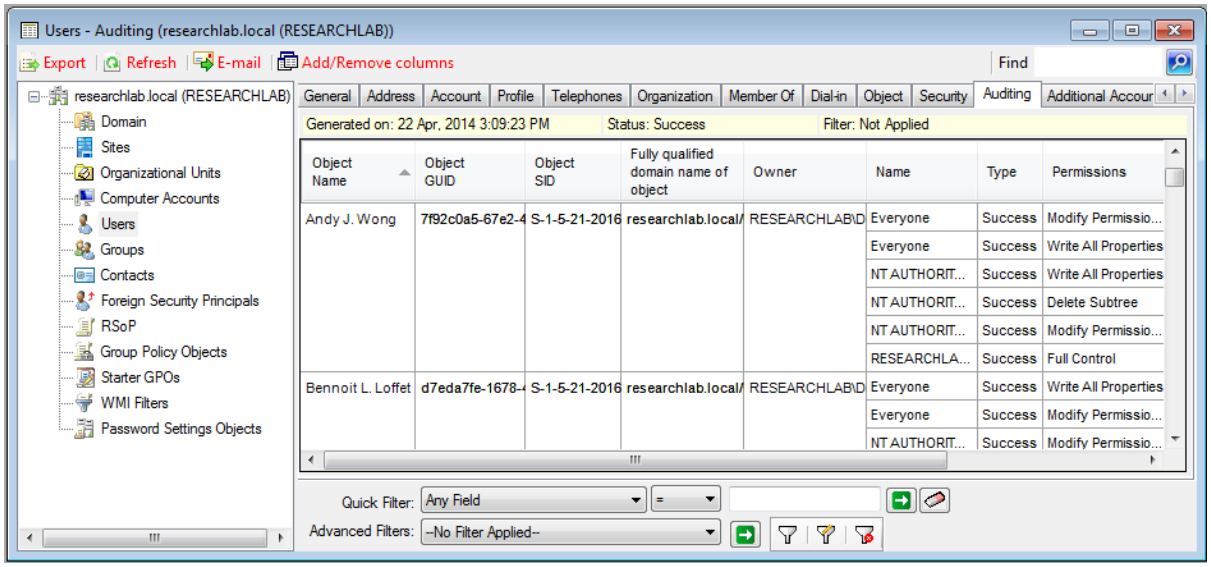
Click on Security tab to view the following information: **{Object Name, Object GUID, and Object SID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



Click on Auditing tab to view the following information: **{Object Name, Object GUID, and Object SID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

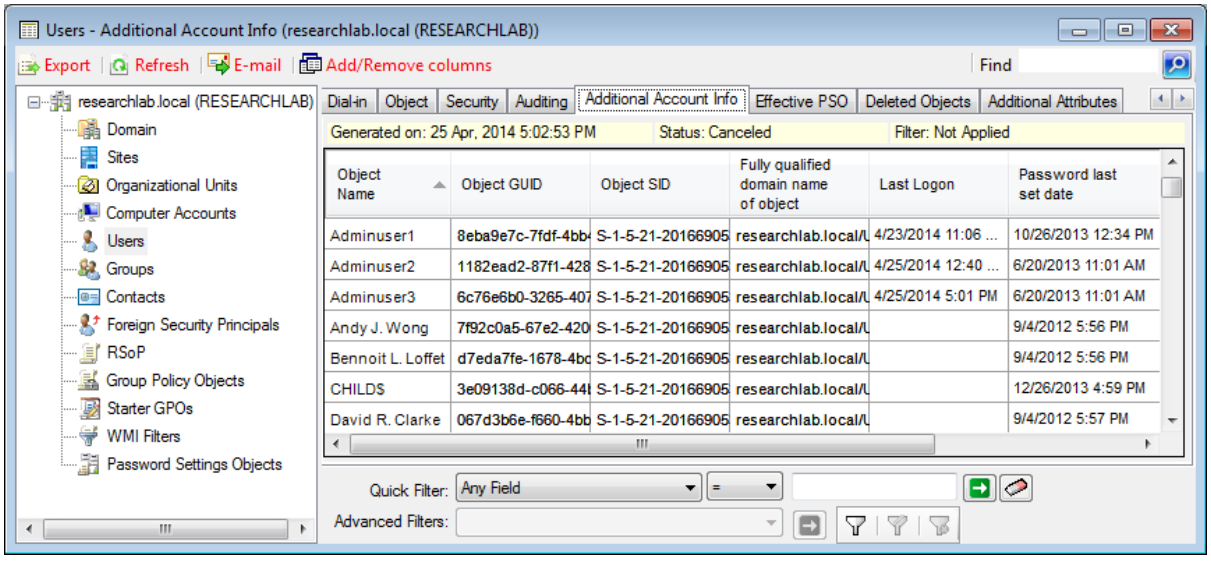
The output would be displayed as shown below:



Click on Additional Account Info tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Last Logon, Password last set date, Password expiration date}.**

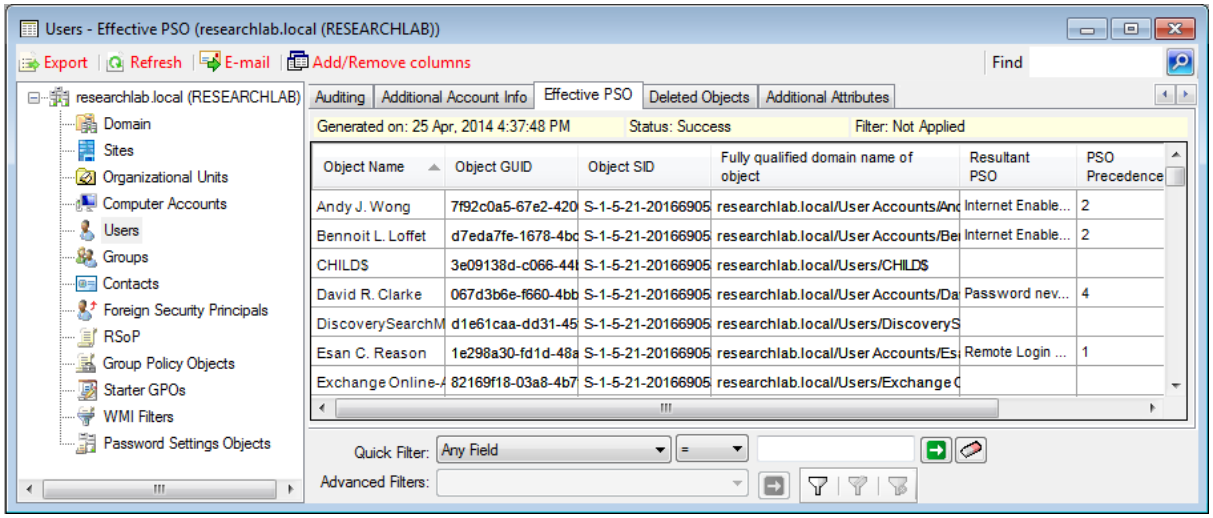
NOTE: ARKAD calculates the last logon date and time by adding the local time zone information. This time zone information is retrieved from the local computer on which ARKAD is run. Also, last logon value for a user can be displayed as empty value if it is not set in the directory or if the current user context or specified user context does not have sufficient privileges to read the attribute from the directory.

The output would be displayed as shown below:



Click on Effective PSO (Win 2008) tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Resultant PSO, PSO Precedence, PSO Description}.**

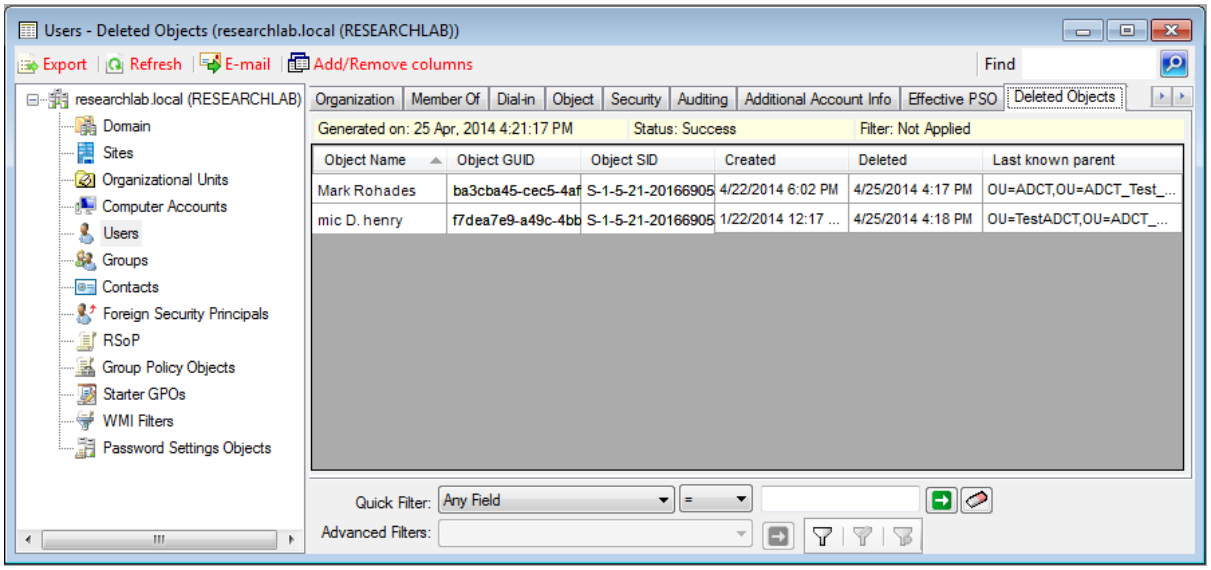
The output would be displayed as shown below:



NOTE: **Effective PSO (Win 2008)** report is applicable only for *Windows Server 2008.*

Click on Deleted Objects tab to view the following information: **{Object Name, Object GUID, Object SID, Created, Deleted, Last known parent}.**

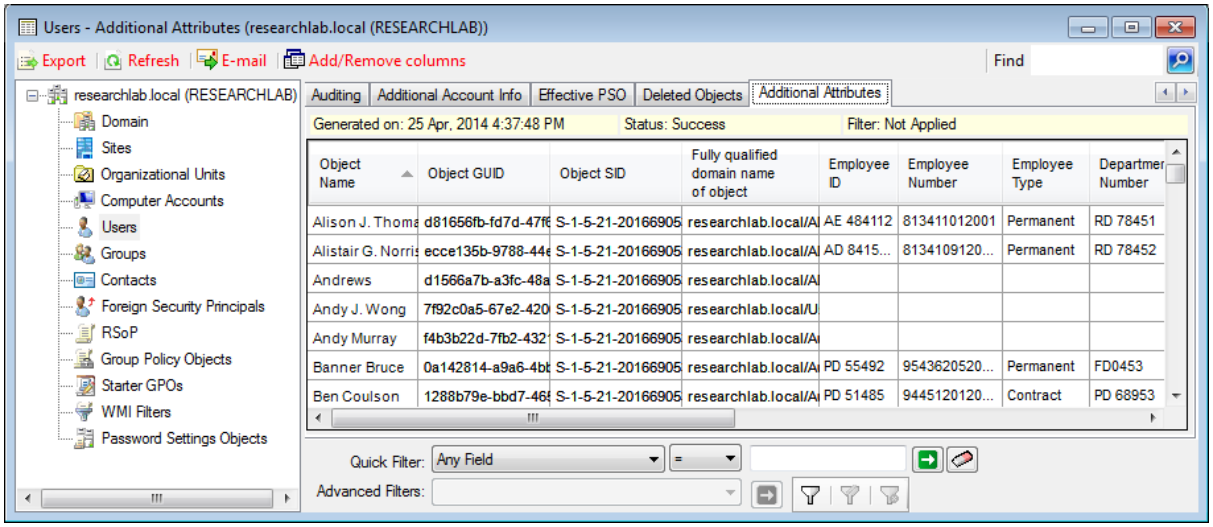
The output would be displayed as shown below:



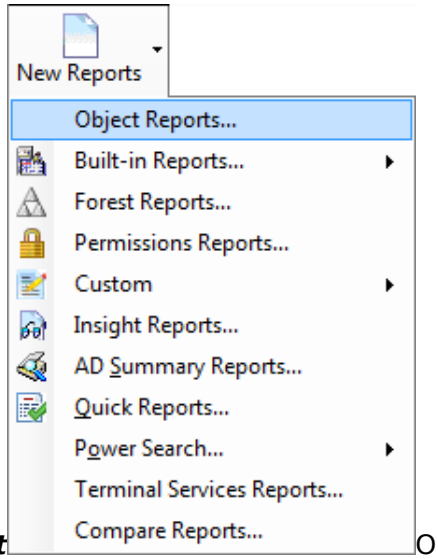
NOTE: The *"Last known parent"* attribute would be set only on a *Windows Server 2003* domain controller and later.

Click Additional Attributes on tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Employee ID, Employee Number, Employee Type, Department Number, Division, Car License, House Identifier, Room Number, Assistant, Secretary}.**

The output would be displayed as shown below:


Users - Additional Attributes (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Add/Remove columns
Find
researchlab.local (RESEARCHLAB)
Domain
Sites
Organizational Units
Computer Accounts
Users
Groups
Contacts
Foreign Security Principals
RSoP
Group Policy Objects
Starter GPOs
WMI Filters
Password Settings Objects
Auditing
Additional Account Info
Effective PSO
Deleted Objects
Additional Attributes
Generated on: 25 Apr, 2014 4:37:48 PM
Status: Success
Filter: Not Applied
Object Name
Object GUID
Object SID
Fully qualified domain name of object
Employee ID
Employee Number
Employee Type
Departmer Number
Alison J. Thoma
d81656fb-fd7d-47f
S-1-5-21-20166905
researchlab.local/A
AE 484112
813411012001
Permanent
RD 78451
Alistair G. Norris
ecce135b-9788-44
S-1-5-21-20166905
researchlab.local/A
AD 8415...
8134109120...
Permanent
RD 78452
Andrews
d1566a7b-a3fc-48a
S-1-5-21-20166905
researchlab.local/A
Andy J. Wong
7f92c0a5-67e2-420
S-1-5-21-20166905
researchlab.local/U
Andy Murray
f4b3b22d-7fb2-432
S-1-5-21-20166905
researchlab.local/A
Banner Bruce
0a142814-a9a6-4bb
S-1-5-21-20166905
researchlab.local/A
PD 55492
9543620520...
Permanent
FD0453
Ben Coulson
1288b79e-bbd7-465
S-1-5-21-20166905
researchlab.local/A
PD 51485
9445120120...
Contract
PD 68953
Quick Filter:
Any Field
=
Advanced Filters:

3.6 How to view Groups Reports?



Select Option under ***New Report*** button. The *Connection Manager* will appear on the screen, which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

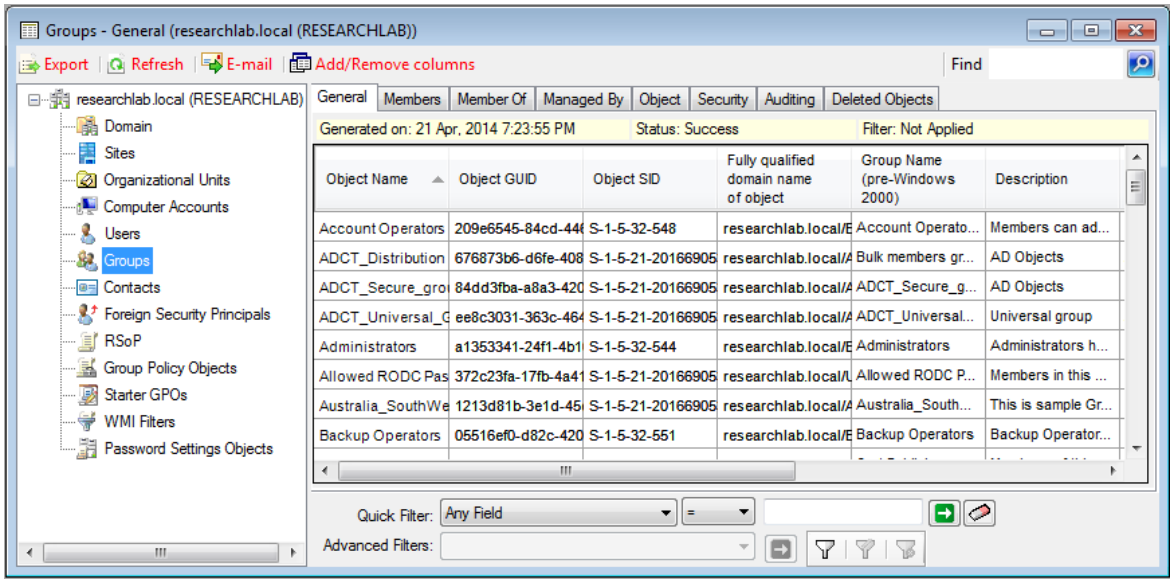
Select and expand the domain node in the left pane of the newly launched report window, and then click on ***Groups***.

Groups report

Click on

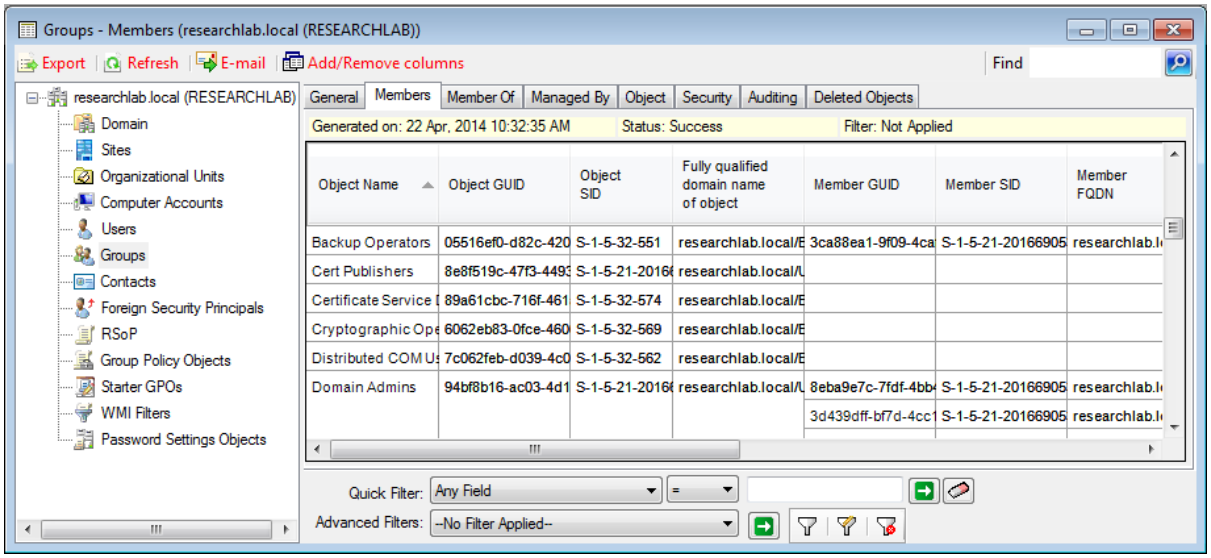
tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Group Name (pre-Windows 2000), Description, E-mail, Group Scope, Group Type, Notes}.**

The output would be displayed as shown below:



Click on tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Member GUID, Member SID, Member FQDN, Members, Sub-group members}.**

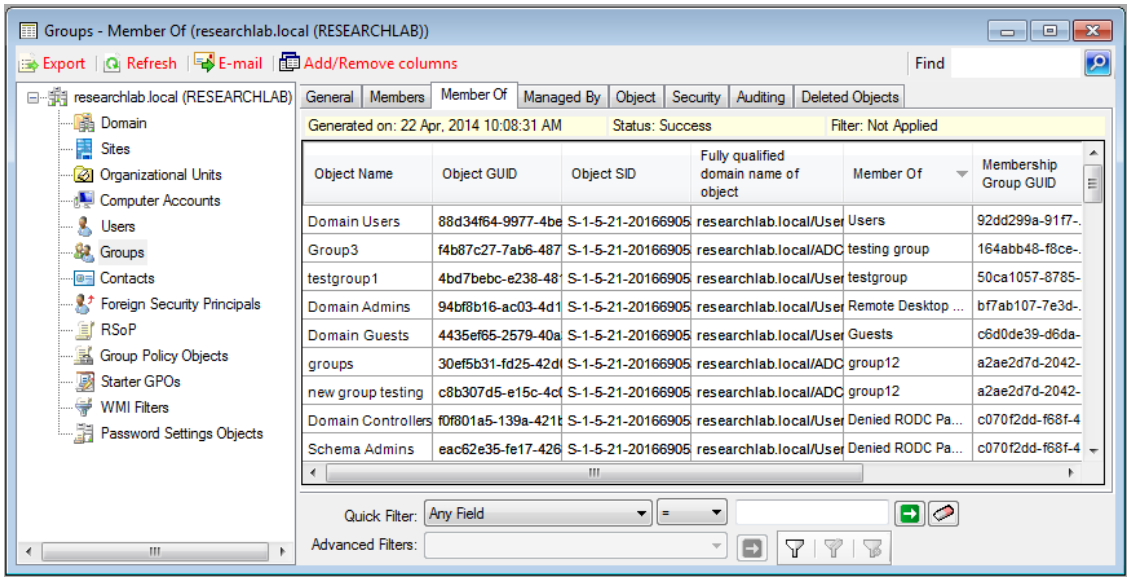
The output would be displayed as shown below:



NOTE: The *"Members"* report shows members of nested groups as well. That is, if Members field in the report contains a group, then its corresponding members would be displayed in Sub-group members' field. Also, the nested group name will appear in the Members field as *"Containing Group\Contained Group".*

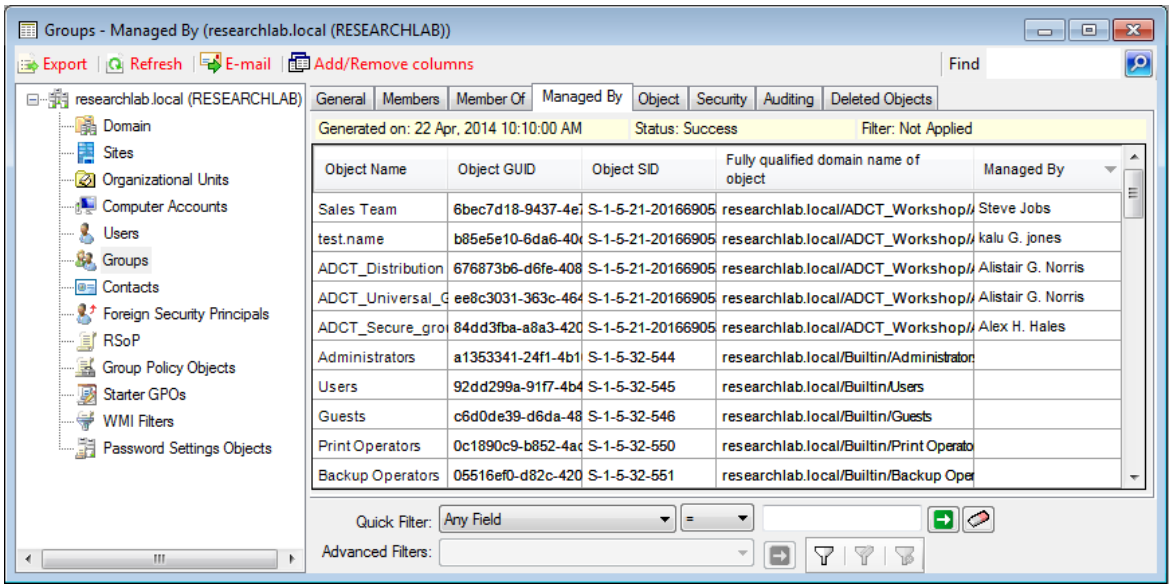
Click on Member Of tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Member Of, Membership Group GUID, Membership Group SID, Membership Group FQDN}.**

The output would be displayed as shown below:



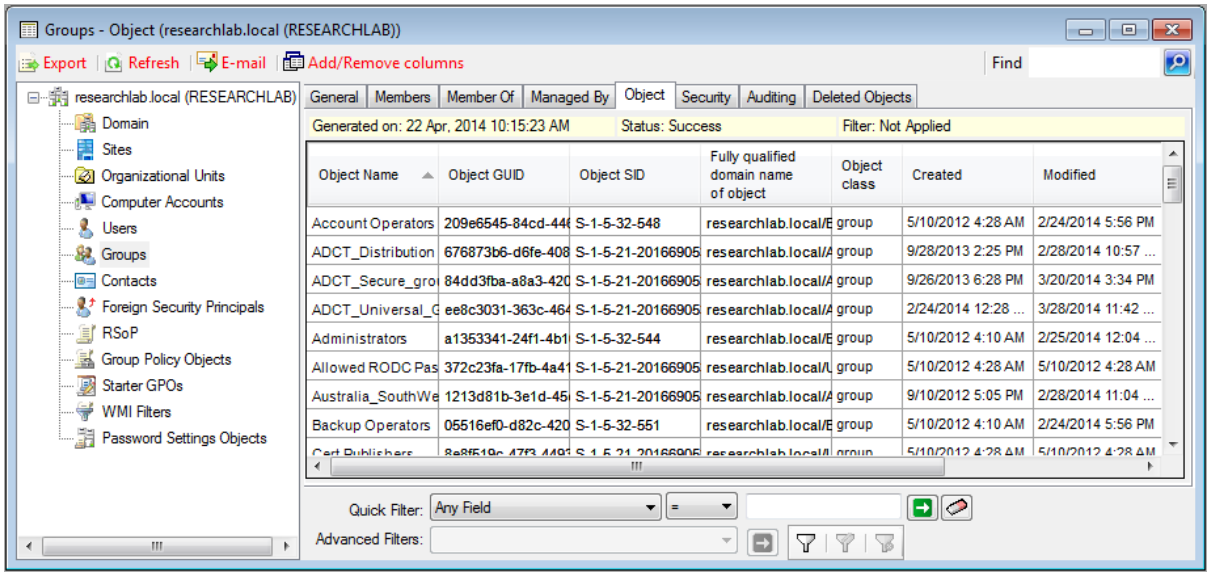
Click on Managed By tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Managed By}.**

The output would be displayed as shown below:



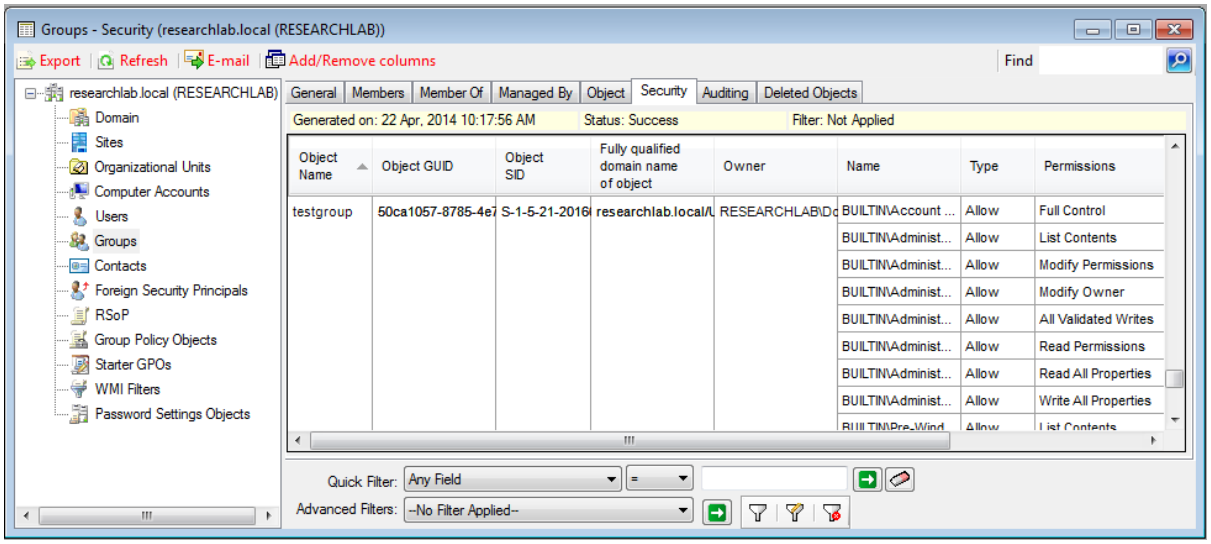
Click on Object tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN}.**

The output would be displayed as shown below:



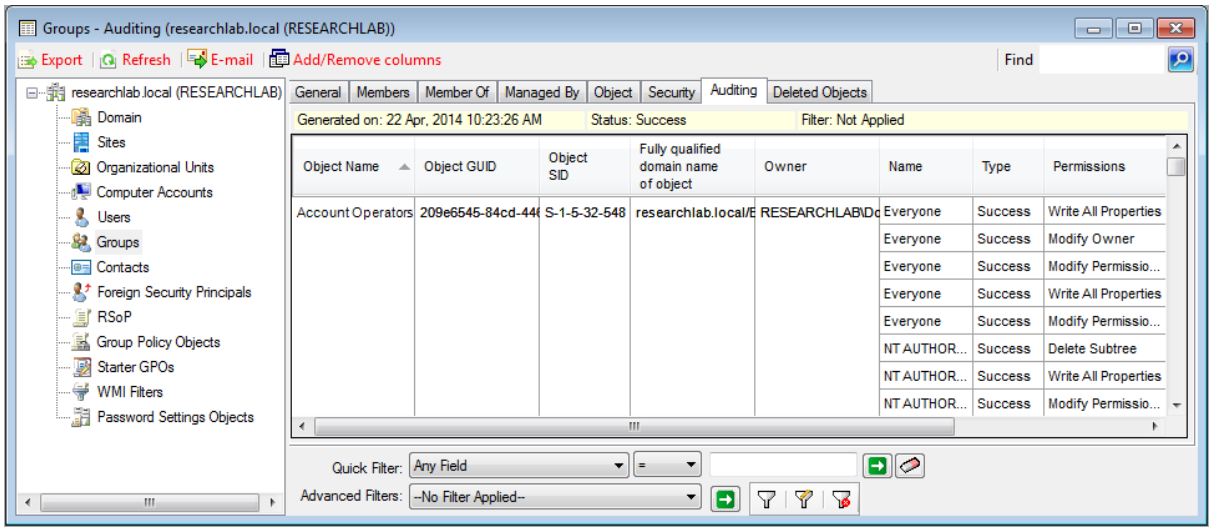
Click on Security tab to view the following information: **{Object Name, Object GUID, Object SID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



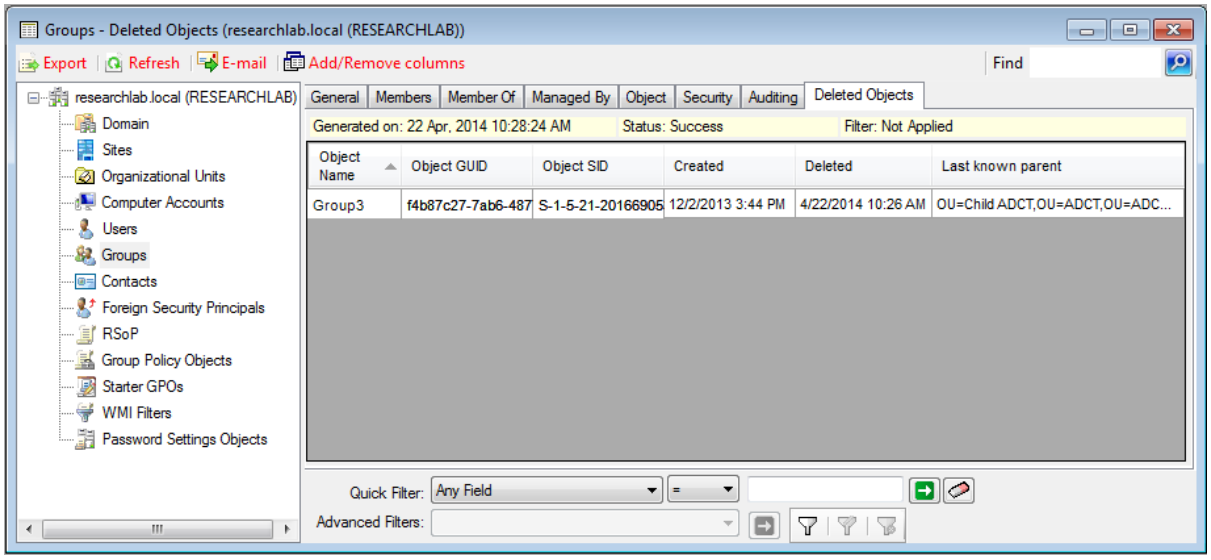
Click on Auditing tab to view the following information: **{Object Name, Object GUID, and Object SID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



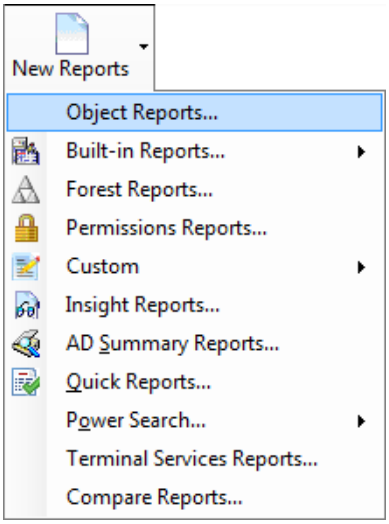
Click on Deleted Objects tab to view the following information: **{Object Name, Object GUID, Object SID, Created, Deleted, Last known parent}.**

The output would be displayed as shown below:



NOTE: The *"Last known parent"* attribute would be set only on a *Windows Server 2003* domain controller and later.

3.7 How to view Contacts Reports?



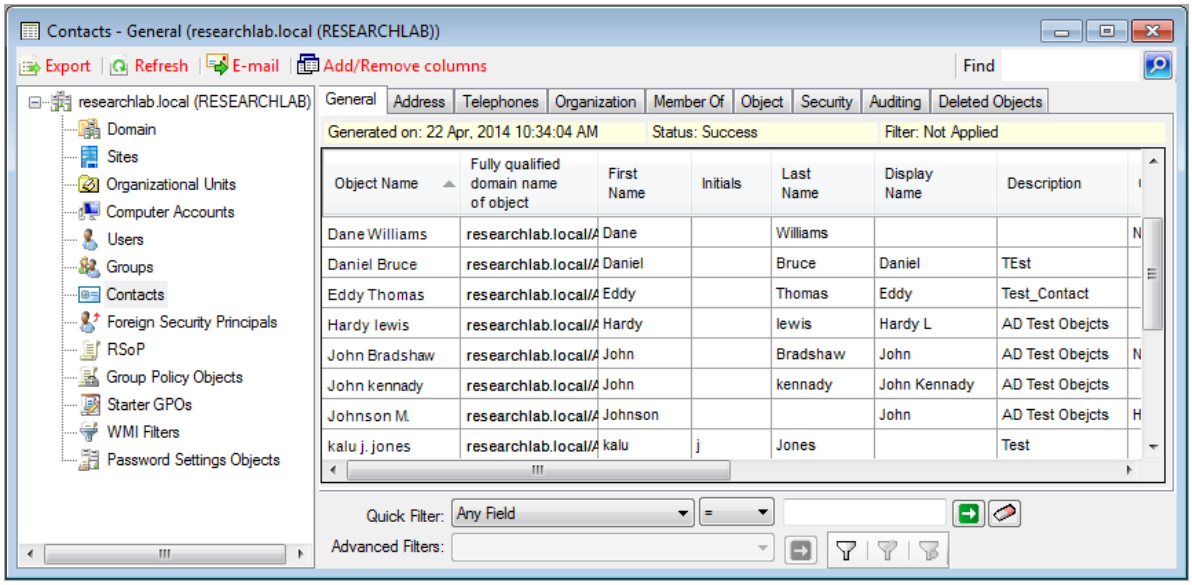
Select option under ***New Report*** button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

Contact report

Click on

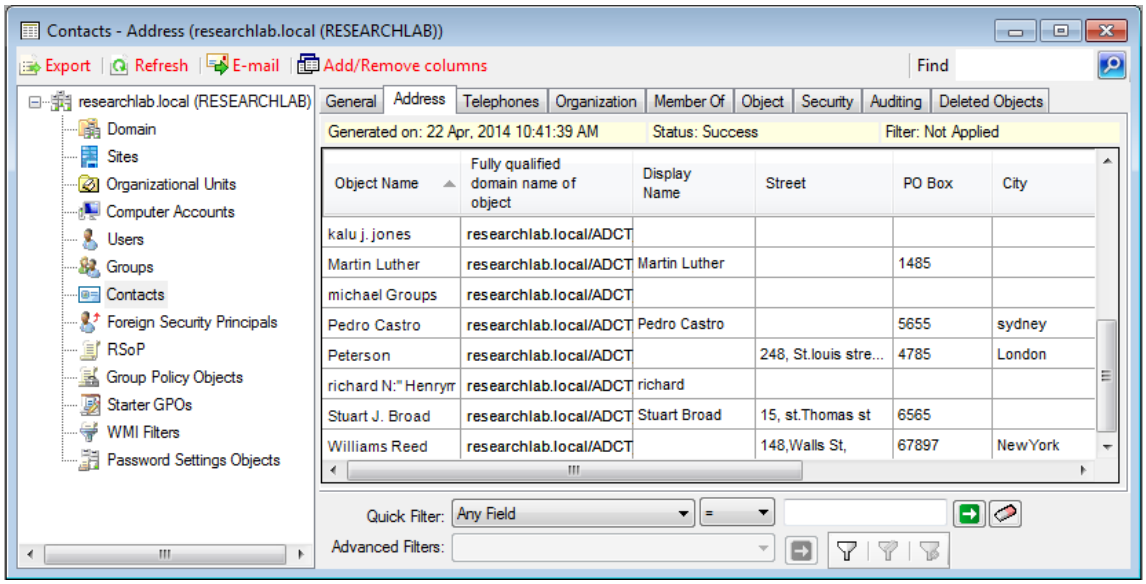
tab to view the following information: **{Object Name, Fully qualified domain name of object, First Name, Initials, Last Name, Display Name, Description, Office, Telephone Number, Phone Numbers (Others), E-mail, Web Page, Web Page Address (Others)}.**

The output would be displayed as shown below:



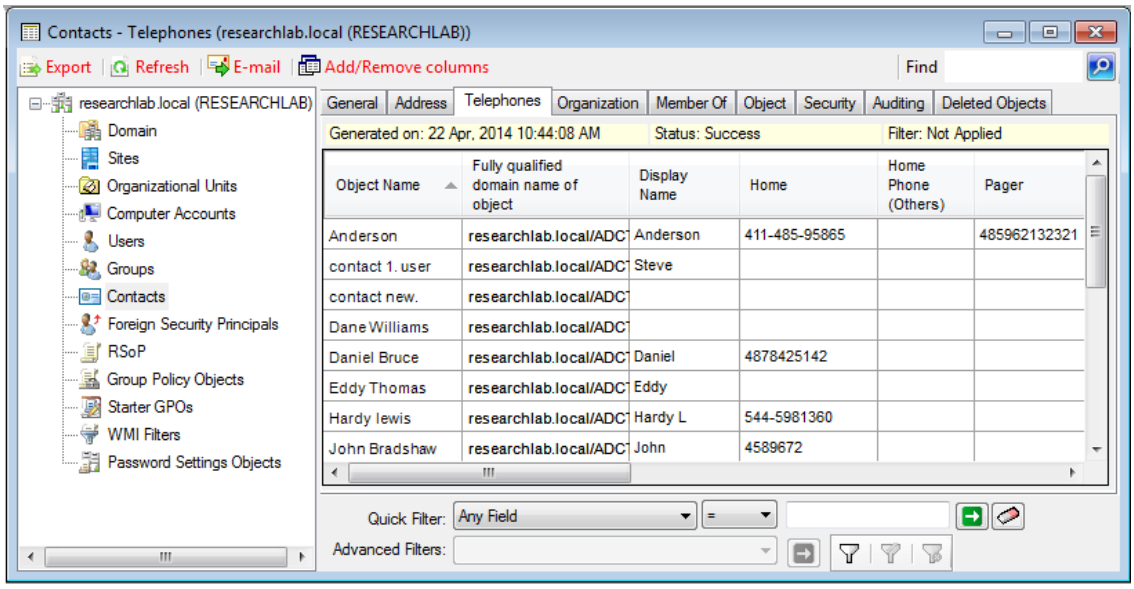
Click on Address tab to view the following information: **{Object Name, Fully qualified domain name of object, Display Name, Street, PO Box, City, State/Province, Zip/Postal Code, and Country/Region}.**

The output would be displayed as shown below:



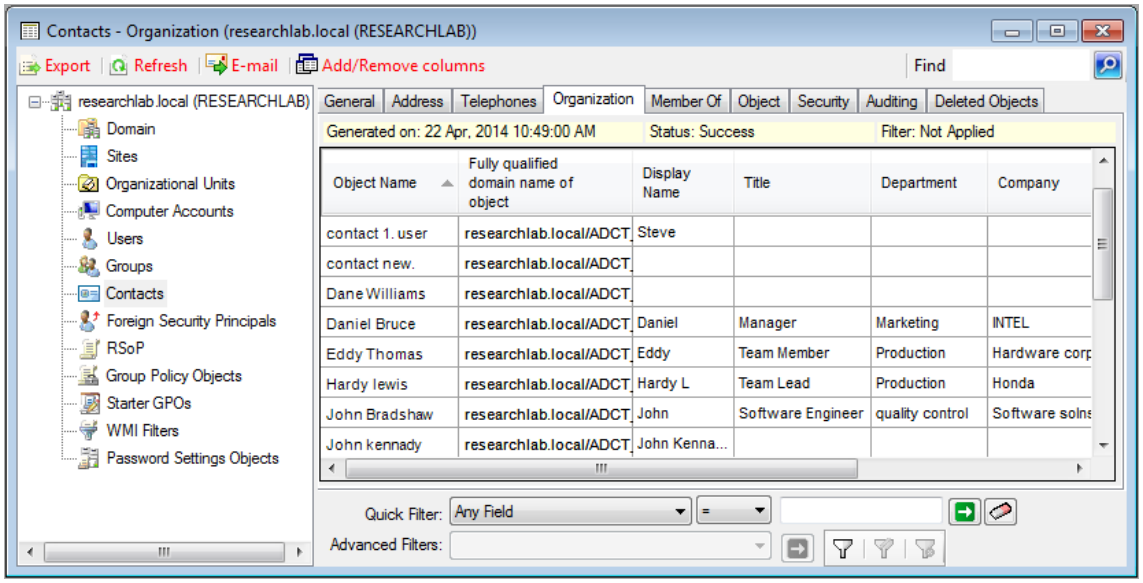
Click on Telephones tab to view the following information: **{Object Name, Fully qualified domain name of object, Display Name, Home, Home Phone (Others), Pager, Pager Number (Others), Mobile, Mobile Number (Others), Fax, Fax Number (Others), IP Phone, IP Phone Number (Others), Notes}.**

The output would be displayed as shown below:



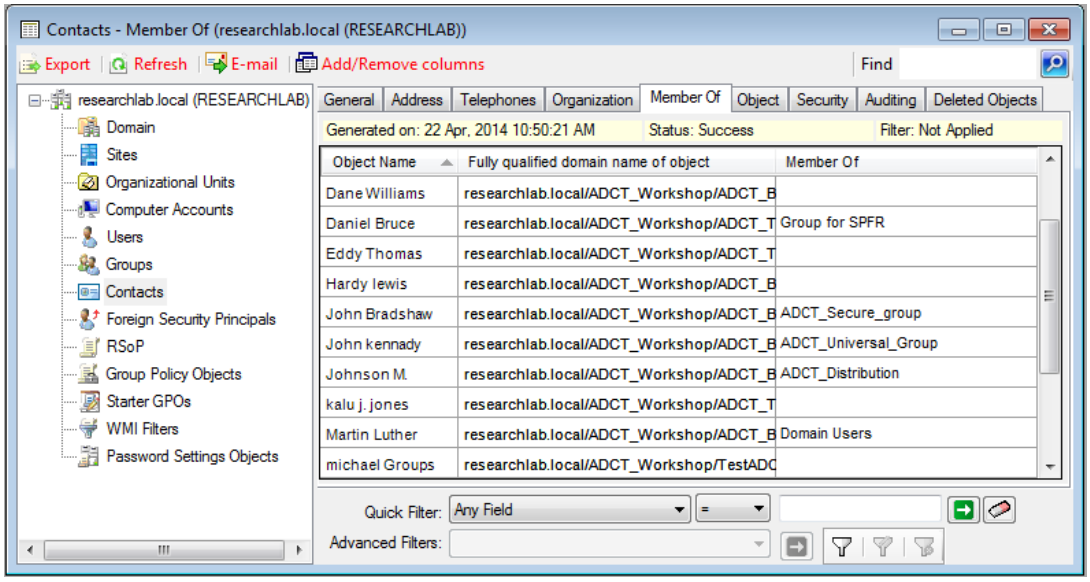
Click on Organization tab to view the following information: **{Object Name, Fully qualified domain name of object, Display Name, Title, Department, Company, Manager, Direct Reports}.**

The output would be displayed as shown below:



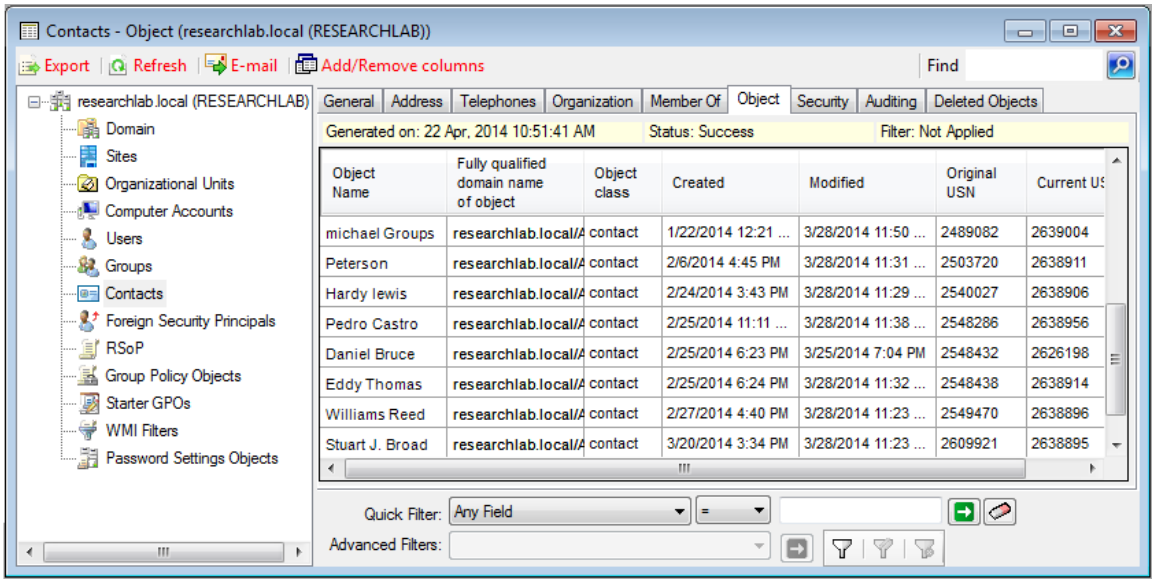
Click on Member Of tab to view the following information: **{Object Name, Fully qualified domain name of object, Member Of, Primary group name}.**

The output would be displayed as shown below:



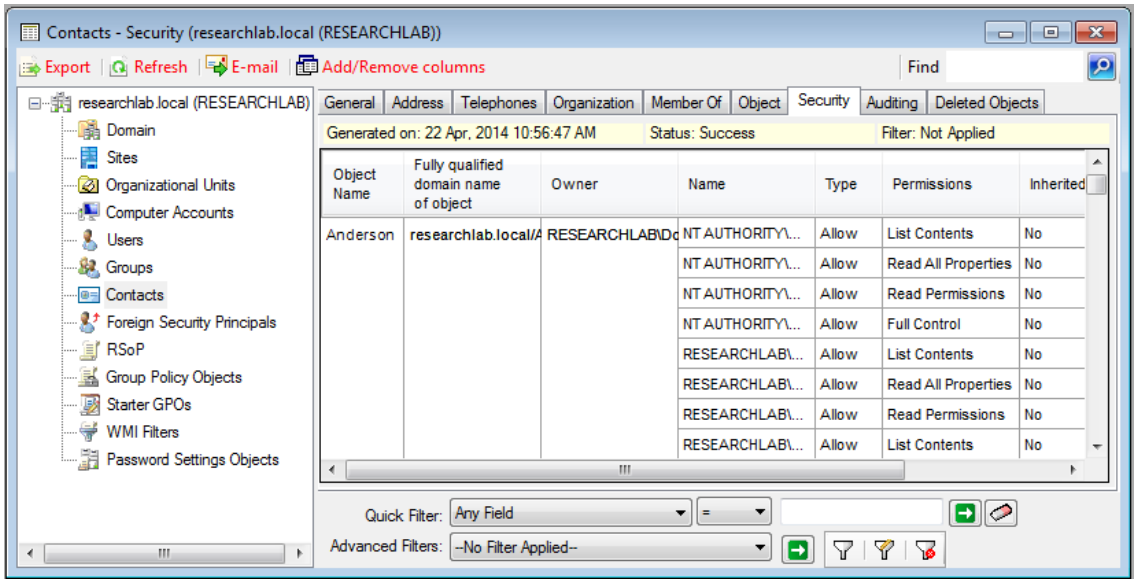
Click on Object tab to view the following information: **{Object Name, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN}.**

The output would be displayed as shown below:



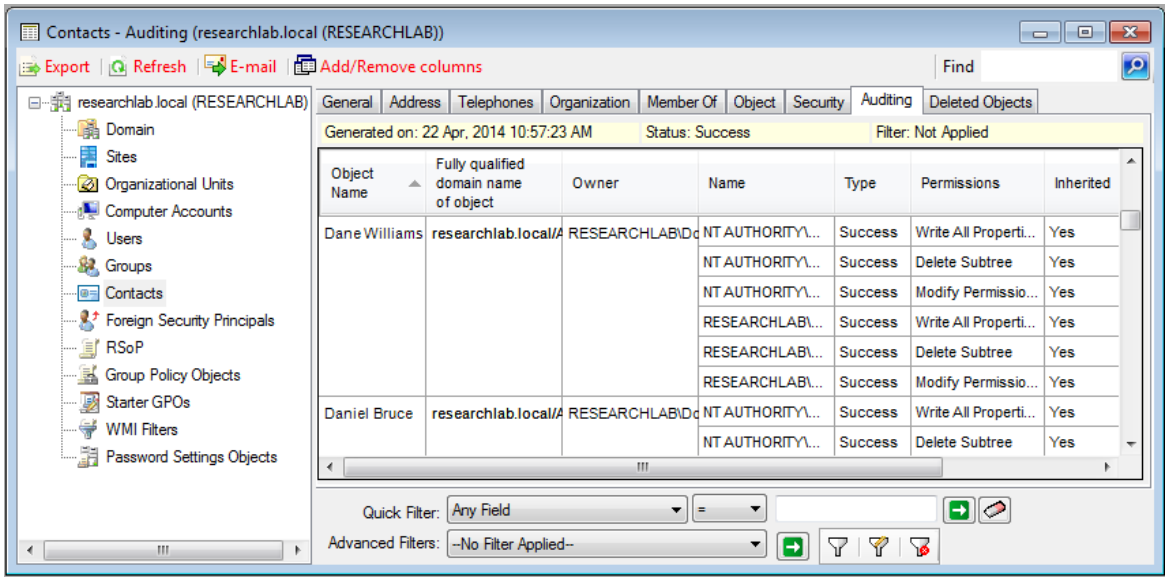
Click on Security tab to view the following information: {Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.

The output would be displayed as shown below:



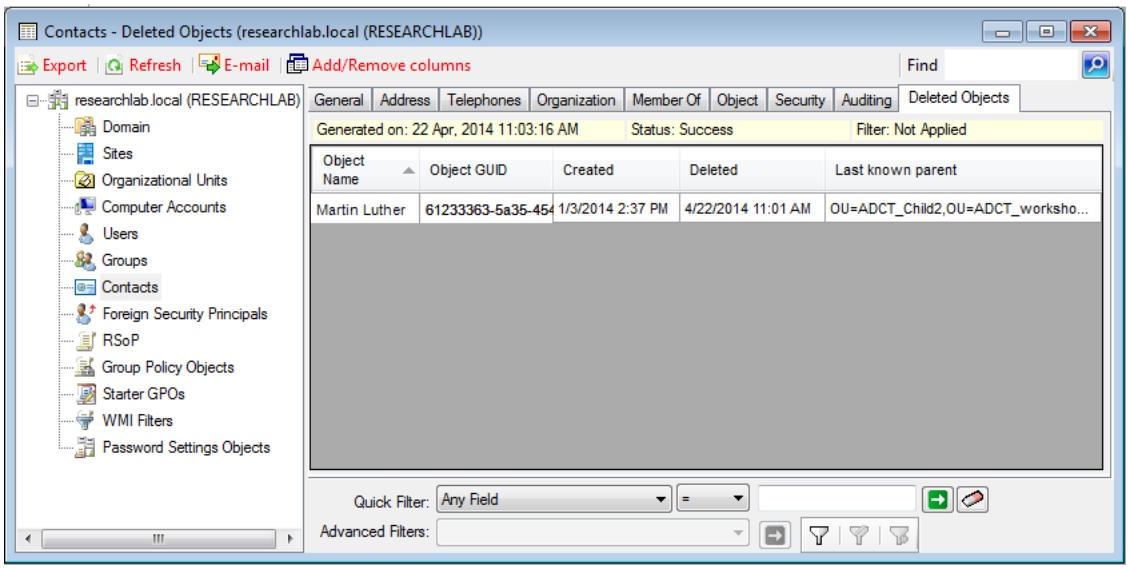
Click on tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



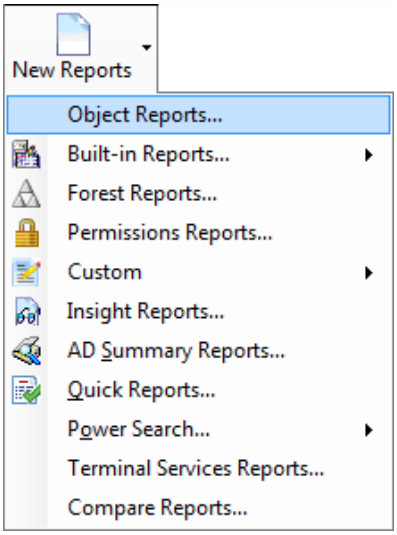
Click on tab to view the following information: **{Object Name, Object GUID, Created, Deleted, Last known parent}.**

The output would be displayed as shown below:



NOTE: The *"Last known parent"* attribute would be set only on a *Windows Server 2003* domain controller and later.

3.8 How to view Foreign Security Principals?



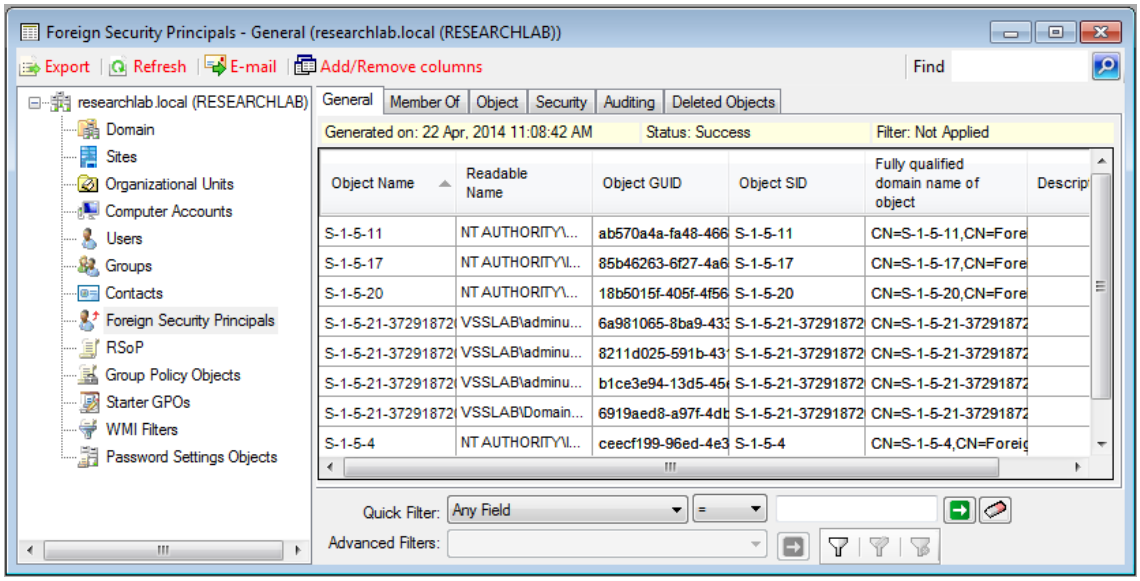
Select option under ***New Report*** button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click on **Foreign Security Principals**.

Foreign Security Principals report

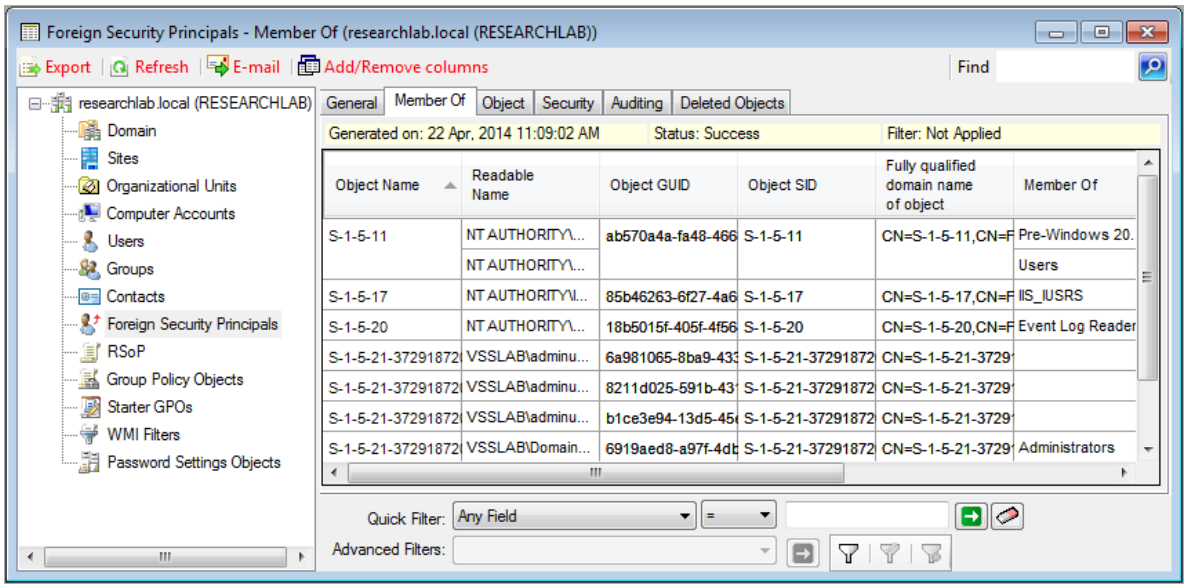
Click on General tab to view the following information: **{Object Name, Readable Name, Object GUID, Object SID, Fully qualified domain name of object, Description}.**

The output would be displayed as shown below:



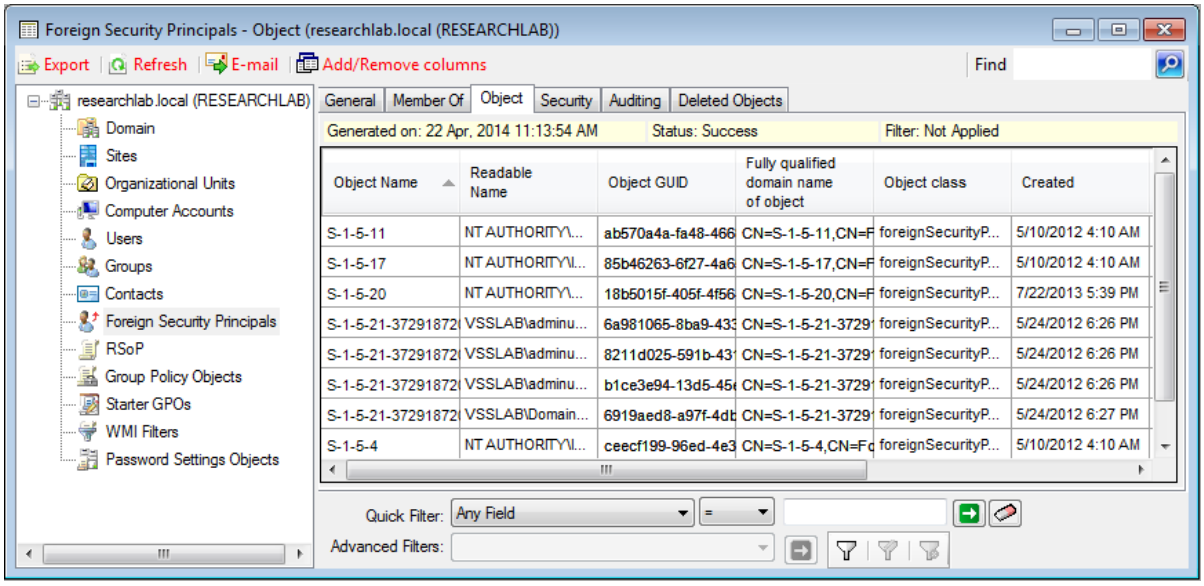
Click on Member Of tab to view the following information: **{Object Name, Readable Name, Object GUID, Object SID, Fully qualified domain name of object, Member Of, Membership Group GUID, Membership Group SID, Membership Group FQDN}.**

The output would be displayed as shown below:



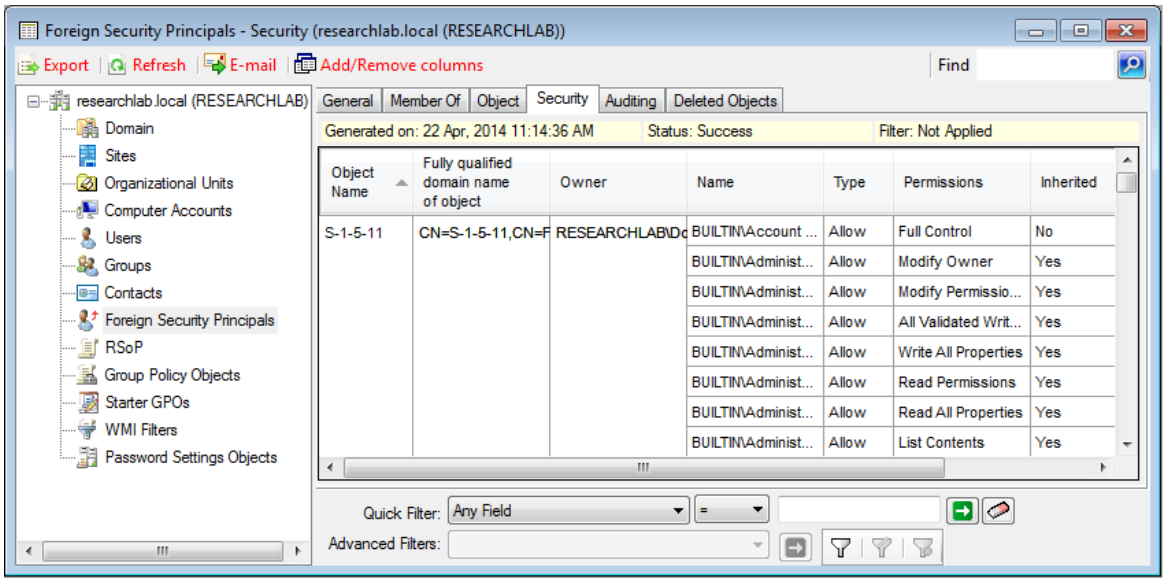
Click on Object tab to view the following information: **{Object Name, Readable Name, Object GUID, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN}.**

The output would be displayed as shown below:



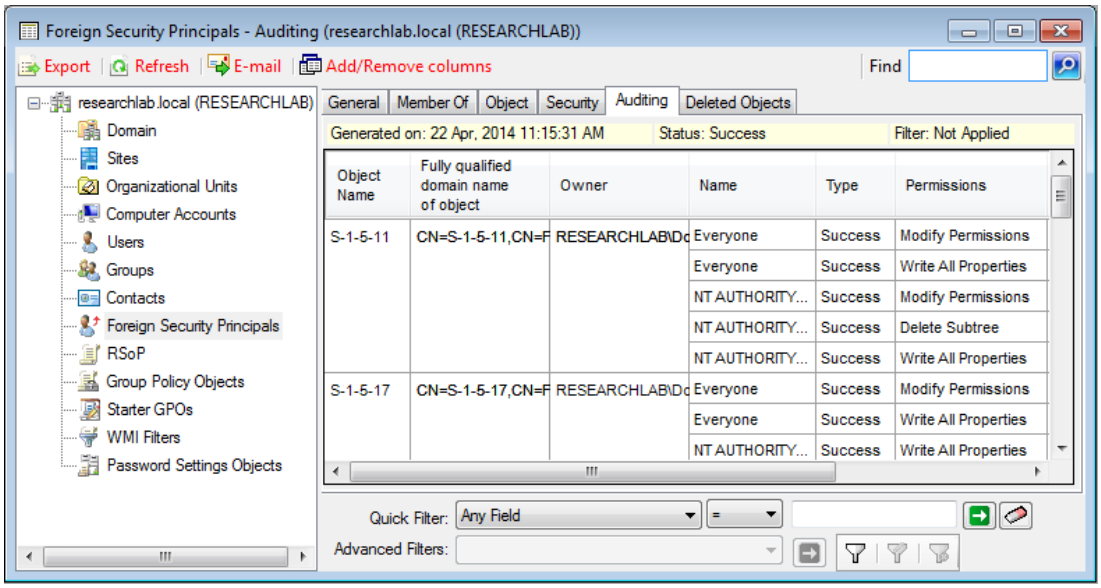
Click on Security tab to view the following information: **{Object Name, Object GUID, and Object SID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



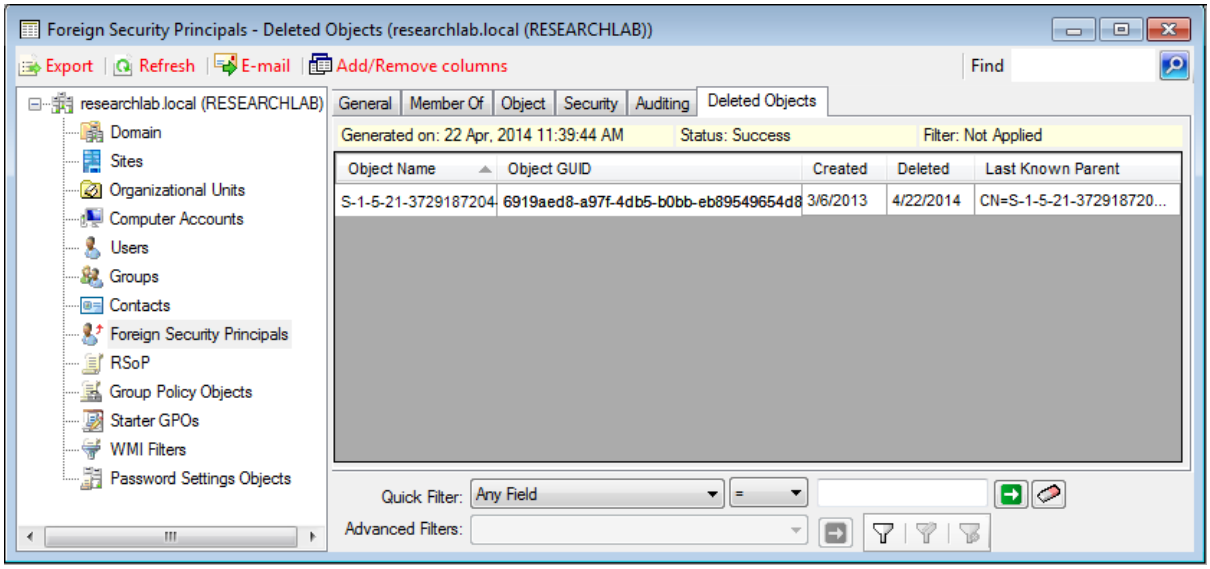
Click on Auditing tab to view the following information: **{Object Name, Object GUID, and Object SID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



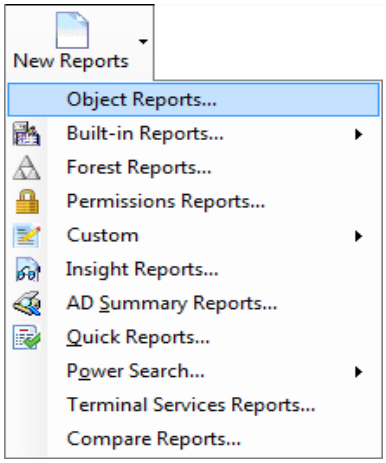
Click on Deleted Objects tab to view the following information: **{Object Name, Object GUID, Object SID, Created, Deleted, Last known parent}.**

The output would be displayed as shown below:



NOTE: The *"Last known parent"* attribute would be set only on a *Windows Server 2003* domain controller and later.

3.9 How to view RSoP Reports?

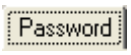


Select *option* under ***New Report*** button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click on **RSoP.**

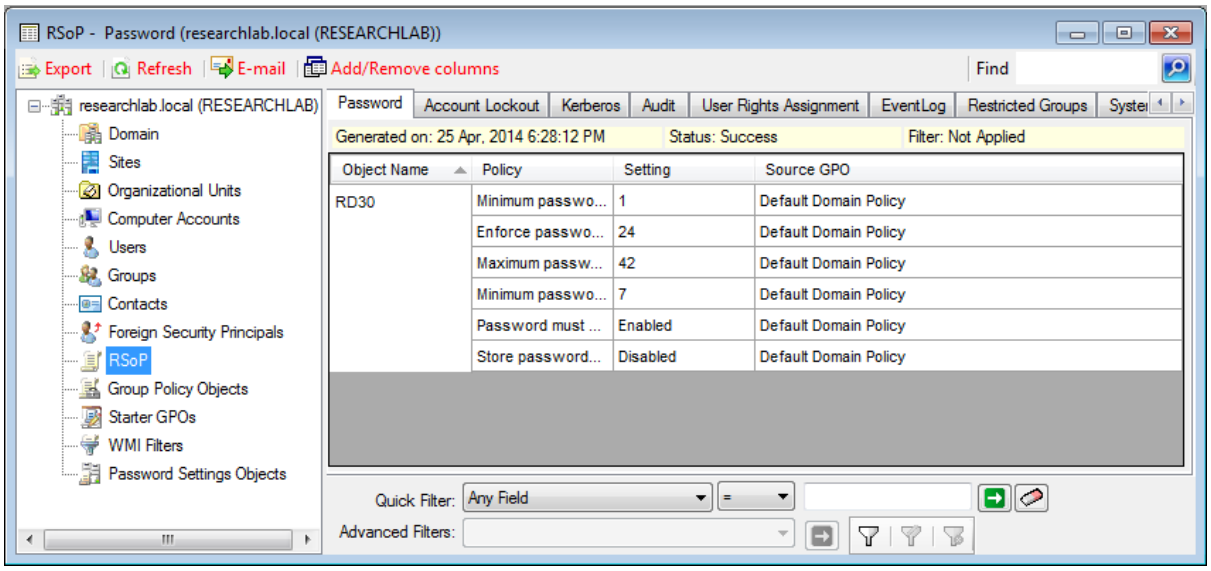
NOTE: RSoP reports can be generated for Domain Controllers running Windows Server 2003 and later.

RSoP report

Click on 

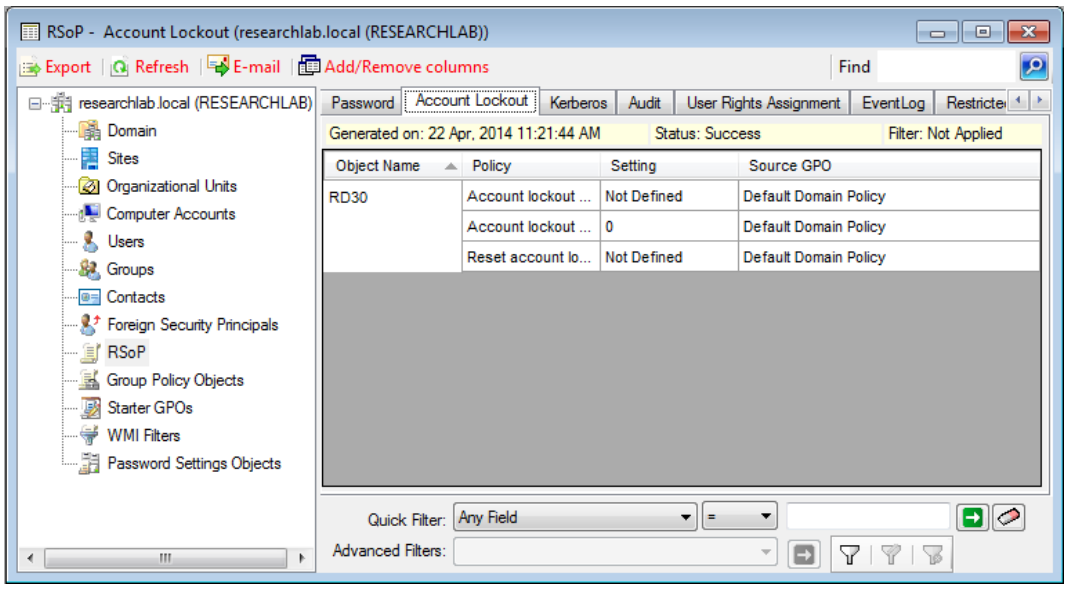
tab to view the following information: **{Object Name, Policy, Setting, and Source GPO}.**

The output would be displayed as shown below:



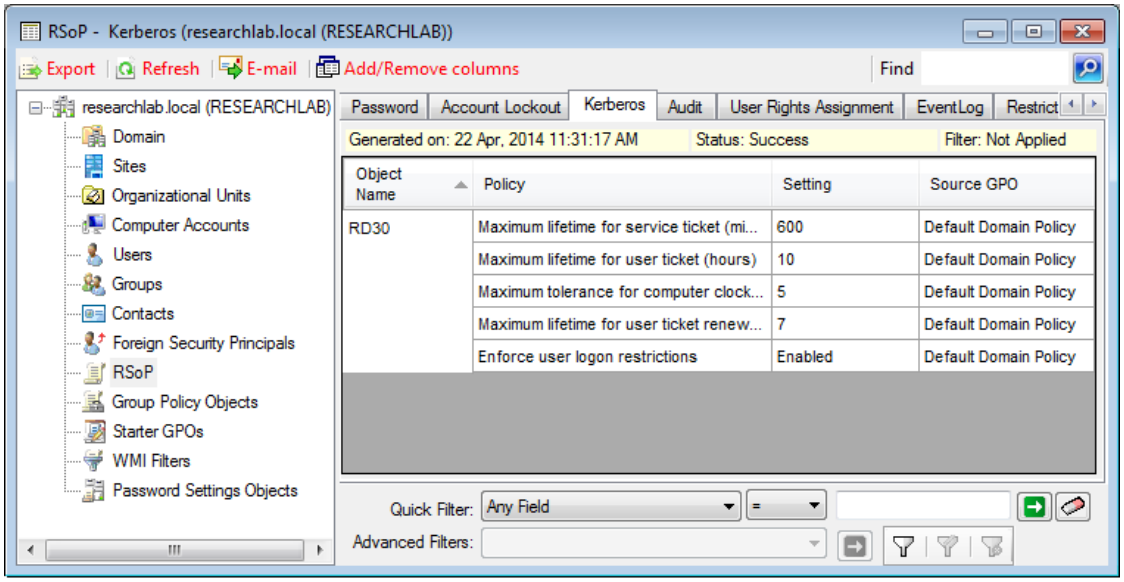
Click on Account Lockout tab to view the following information: **{Object Name, Policy, Setting, and Source GPO}.**

The output would be displayed as shown below:



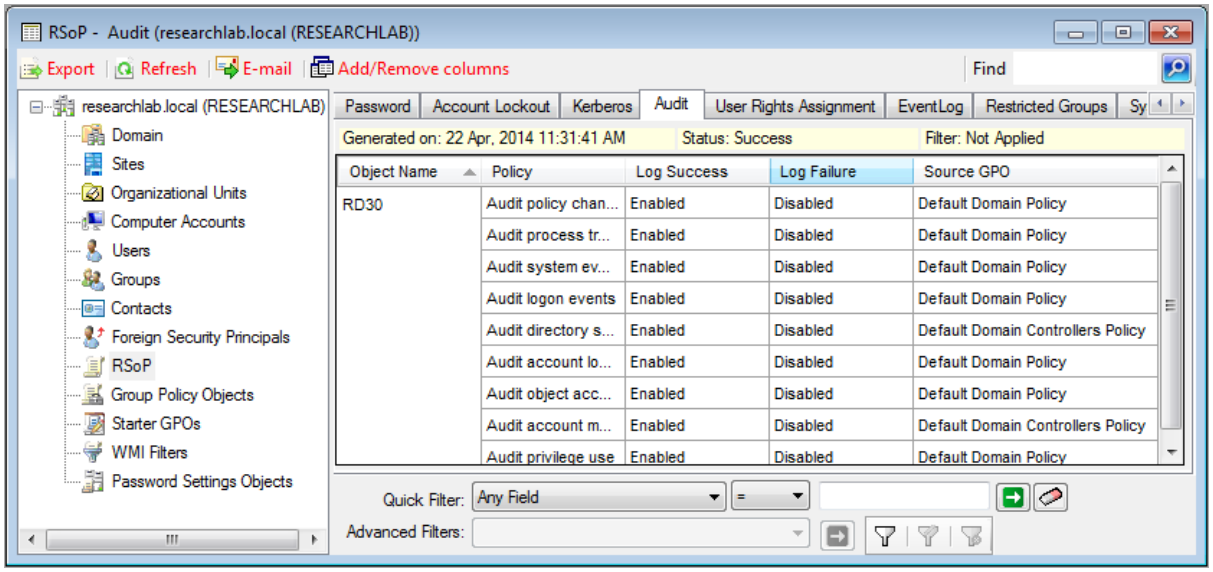
Click on Kerberos tab to view the following information: **{Object Name, Policy, Setting, and Source GPO}.**

The output would be displayed as shown below:



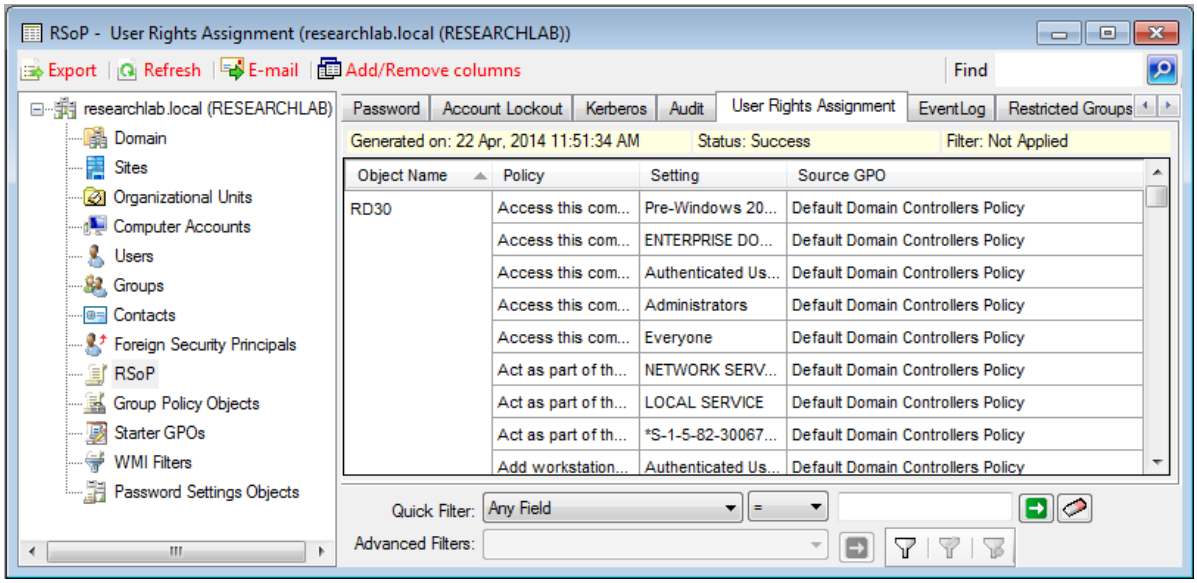
Click on Audit tab to view the following information: **{Object Name, Policy, Log Success, Log Failure, and Source GPO}.**

The output would be displayed as shown below:



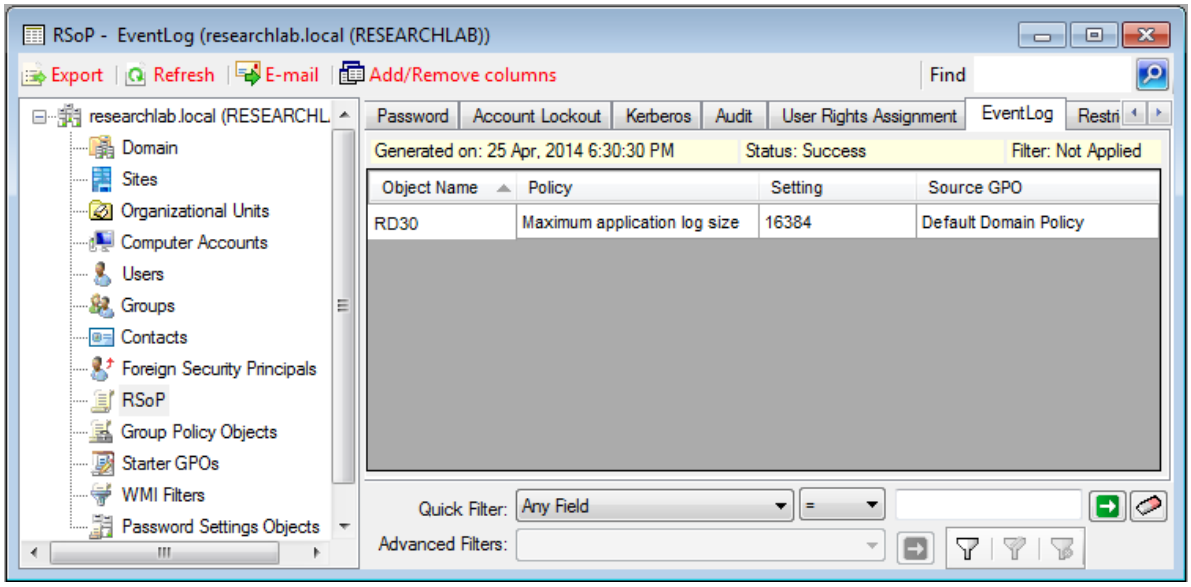
Click on User Rights Assignment tab to view the following information: **{Object Name, Policy, Setting, and Source GPO}.**

The output would be displayed as shown below:



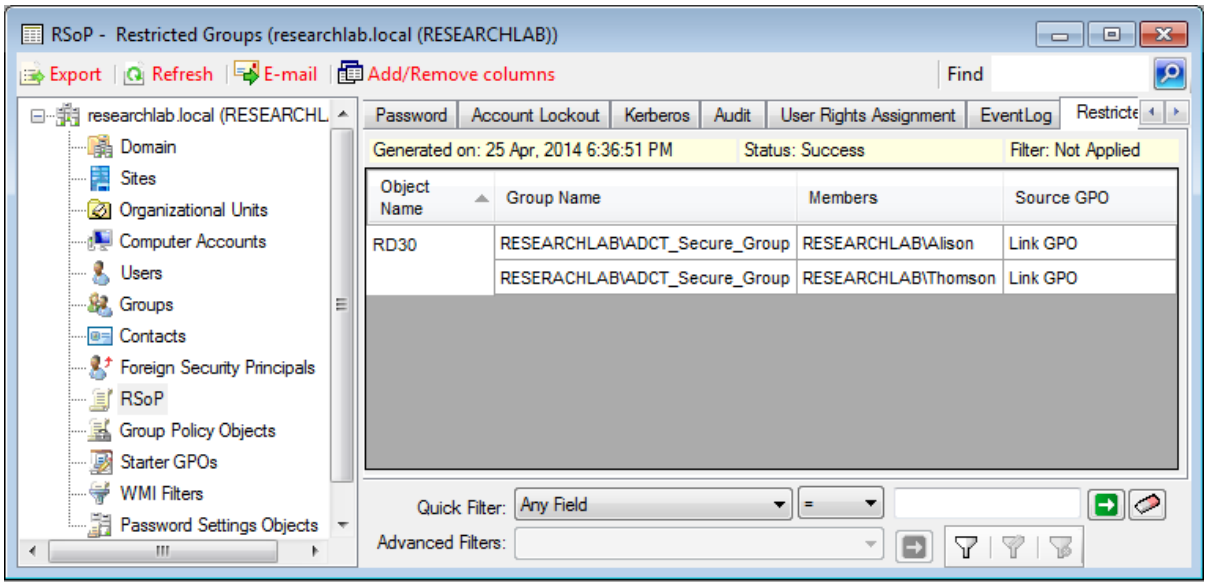
Click on EventLog tab to view the following information: **{Object Name, Policy, Setting, and Source GPO}.**

The output would be displayed as shown below:



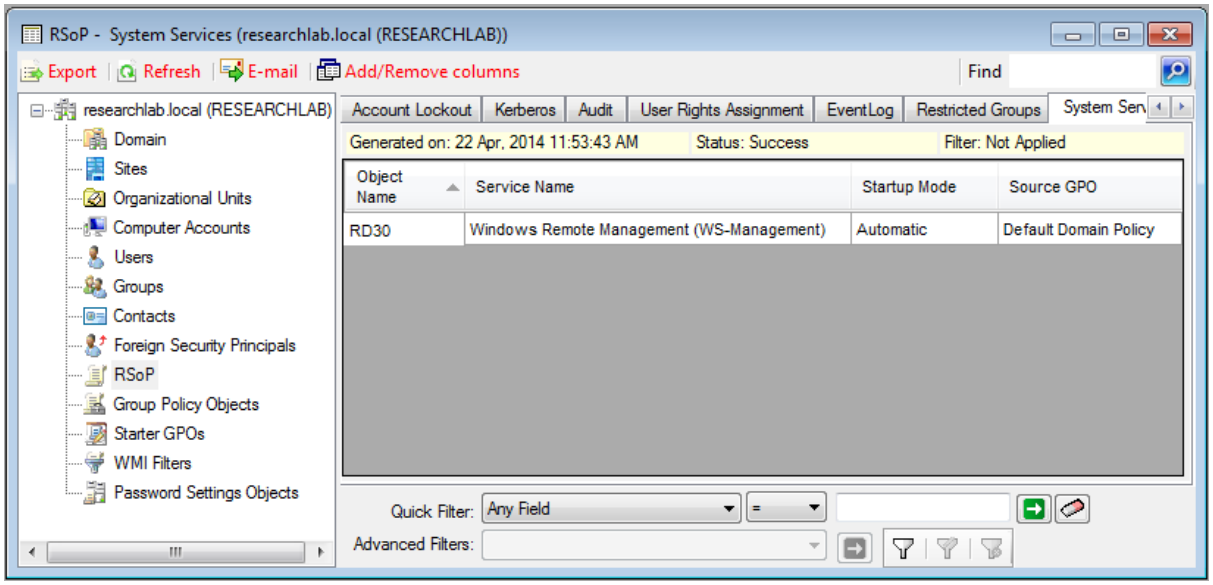
Click on Restricted Groups tab to view the following information: **{Object Name, Group Name, Members, and Source GPO}.**

The output would be displayed as shown below:



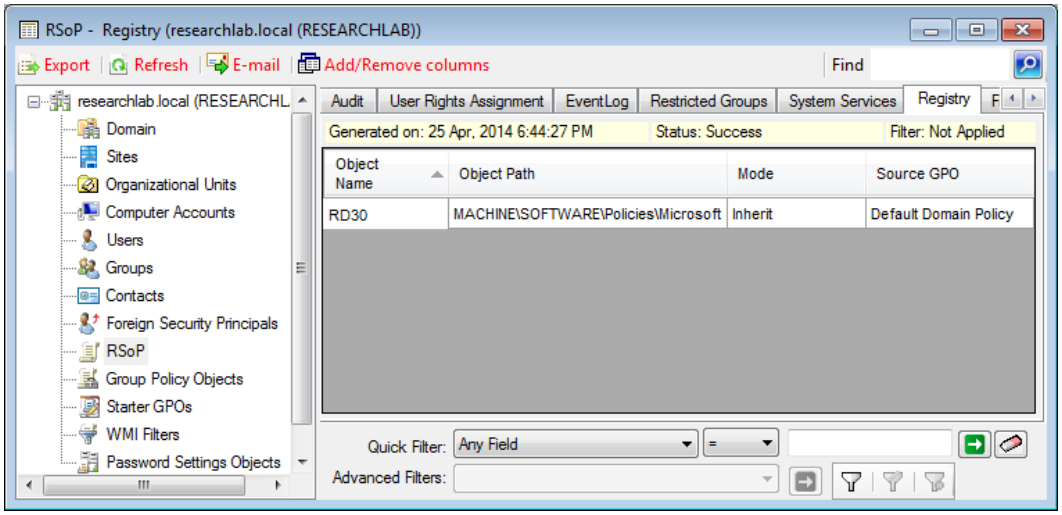
Click on System Services tab to view the following information: **{Object Name, Service Name, Startup Mode, and Source GPO}.**

The output would be displayed as shown below:



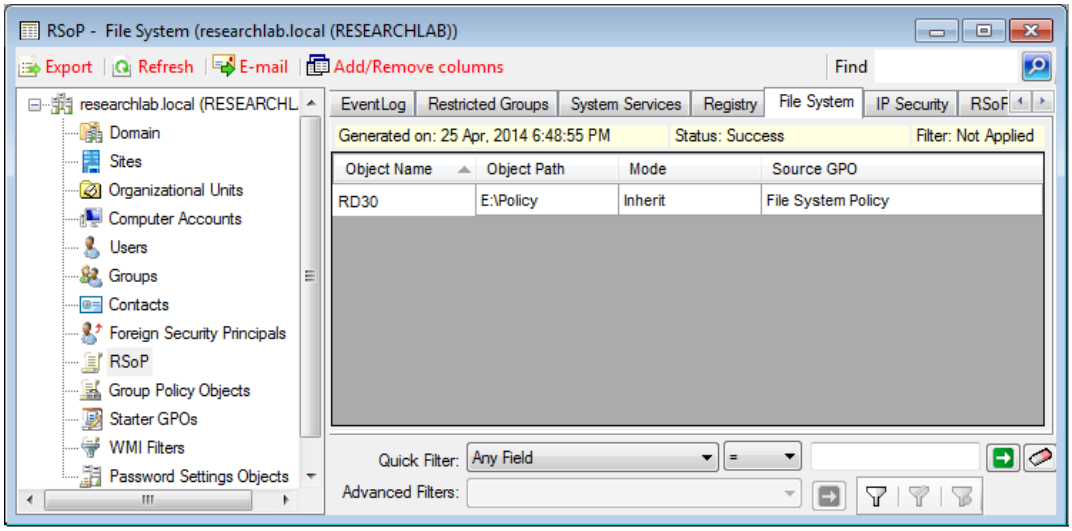
Click on Registry tab to view the following information: **{Object Name, Object Path, Mode, and Source GPO}.**

The output would be displayed as shown below:

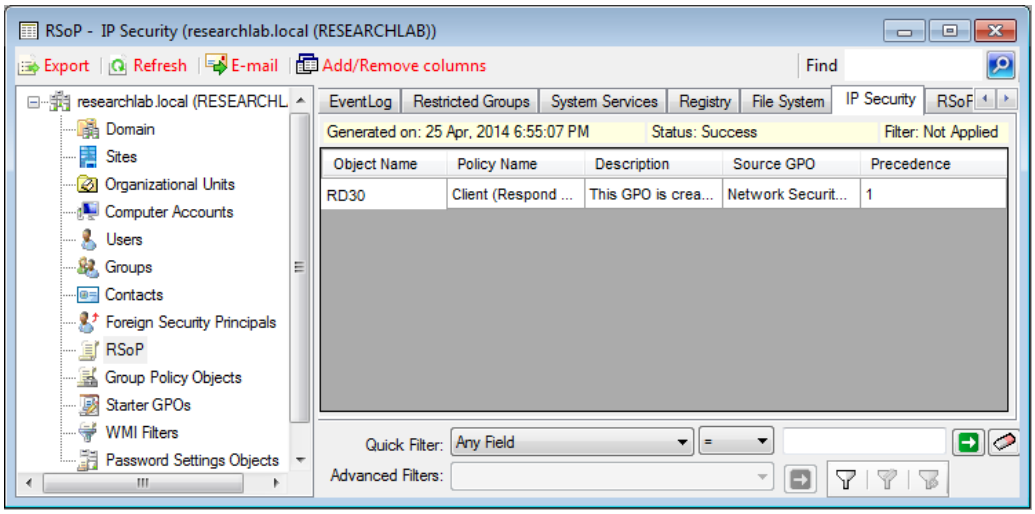


Click on File System tab to view the following information: **{Object Name, Object Path, Mode, and Source GPO}.**

The output would be displayed as shown below:

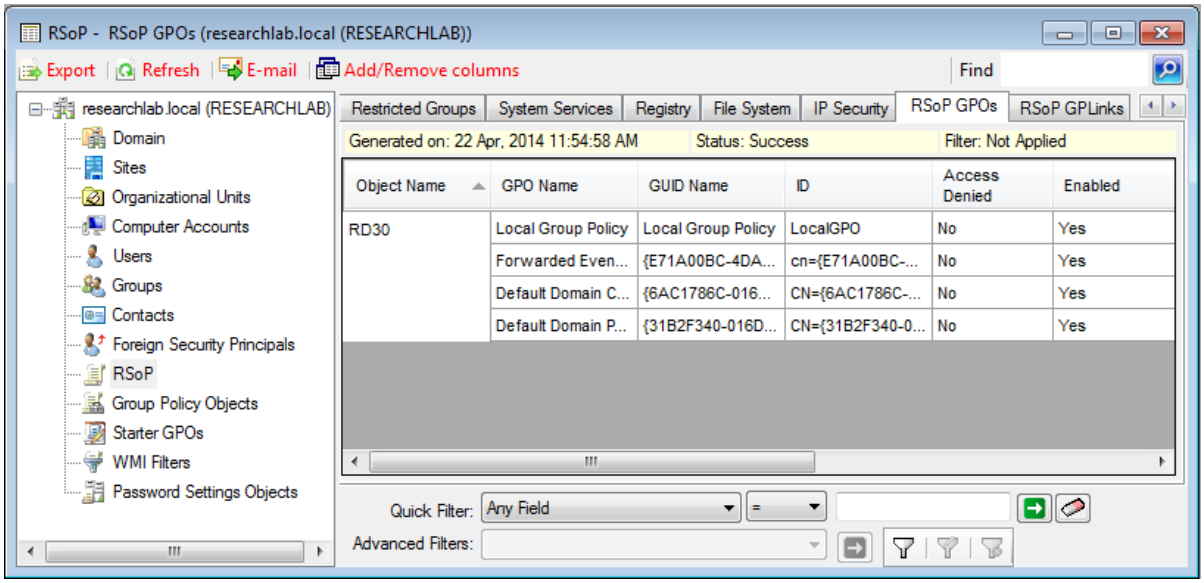


Click on IP Security tab to view the following information: **{Object Name, Policy Name, Description, Source GPO, and Precedence}.**



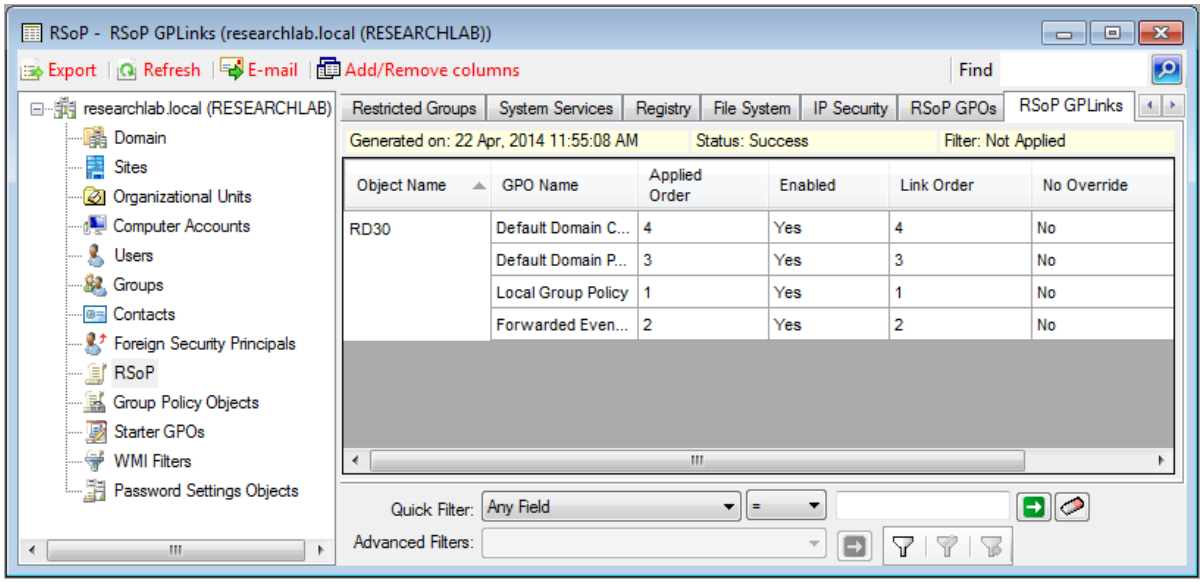
Click on RSoP GPOs tab to view the following information: **{Object Name, GPO Name, GUID Name, ID, Access Denied, Enabled, File System Path, Filter Allowed, WMI Filter ID, and Version}.**

The output would be displayed as shown below:

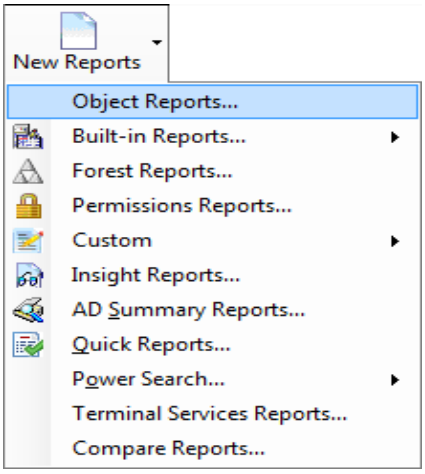


Click on RSoP GPLinks tab to view the following information: **{Object Name, GPO Name, Applied Order, Enabled, Link Order, No Override, and SOM Order}.**

The output would be displayed as shown below:



3.10 How to view Group Policy Object Reports?



Select *option* under ***New Report*** button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click Group Policy Objects.

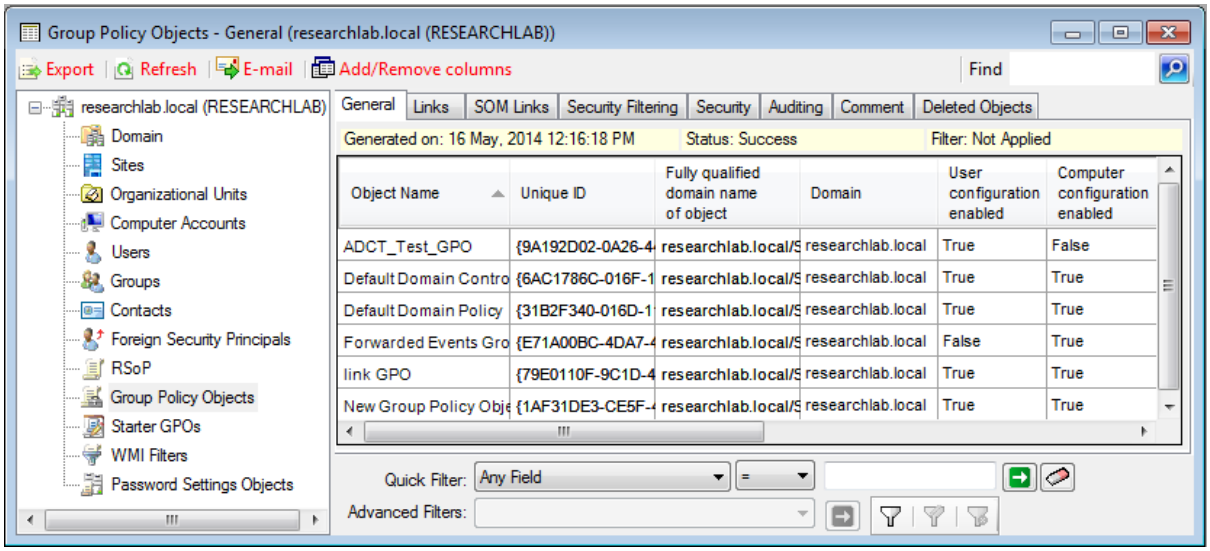
NOTE: Group Policy Object reports require GPMC to be installed on the local computer where ARKAD is running. However, for generating Security, Auditing and Deleted Objects reports GPMC is not required. For Comment (Win 2008) reports, Windows Server 2008 GPMC is installed.

Group Policy Object Report

Click

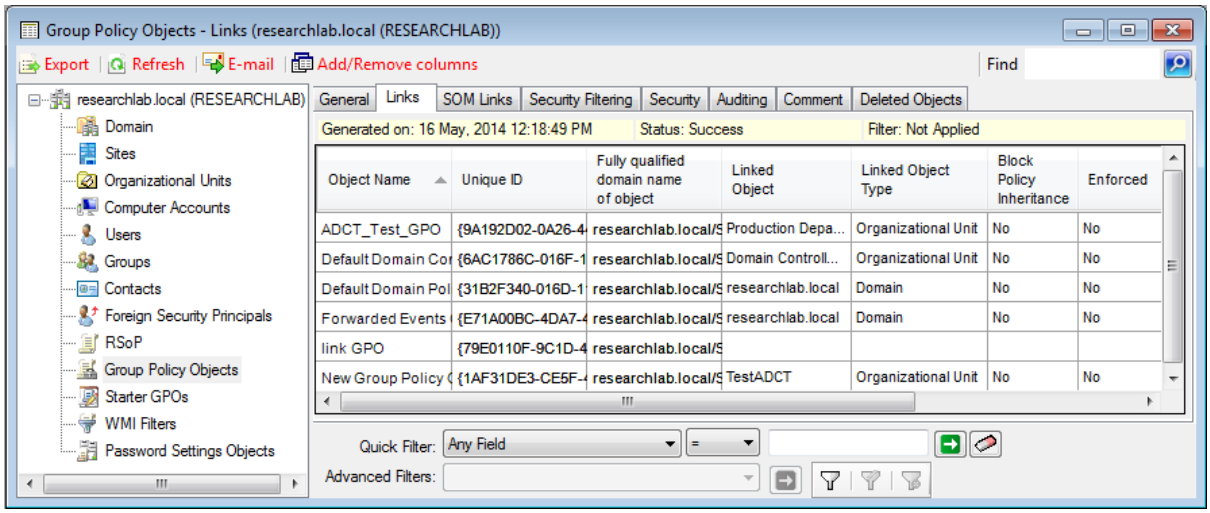
tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Domain, User configuration enabled, Computer configuration enabled, Created, Modified, WMI Filter, User configuration version, Computer configuration version}.**

The output would be displayed as shown below:



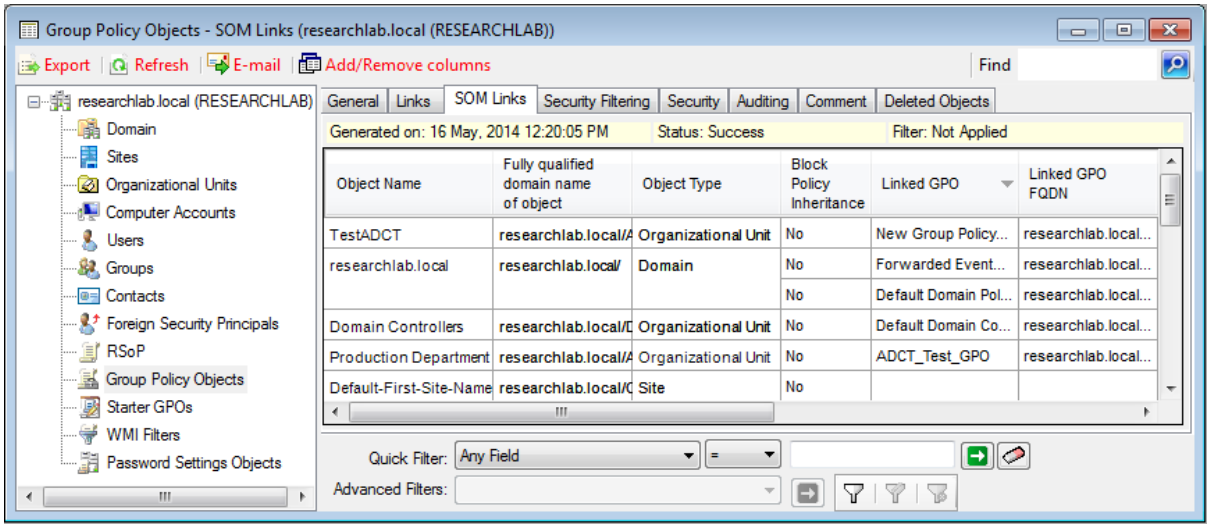
Click on Links tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Linked Object, Linked Object Type, Block Policy Inheritance, Enforced, Link Enabled, Linked Object FQDN}.**

The output would be displayed as shown below:



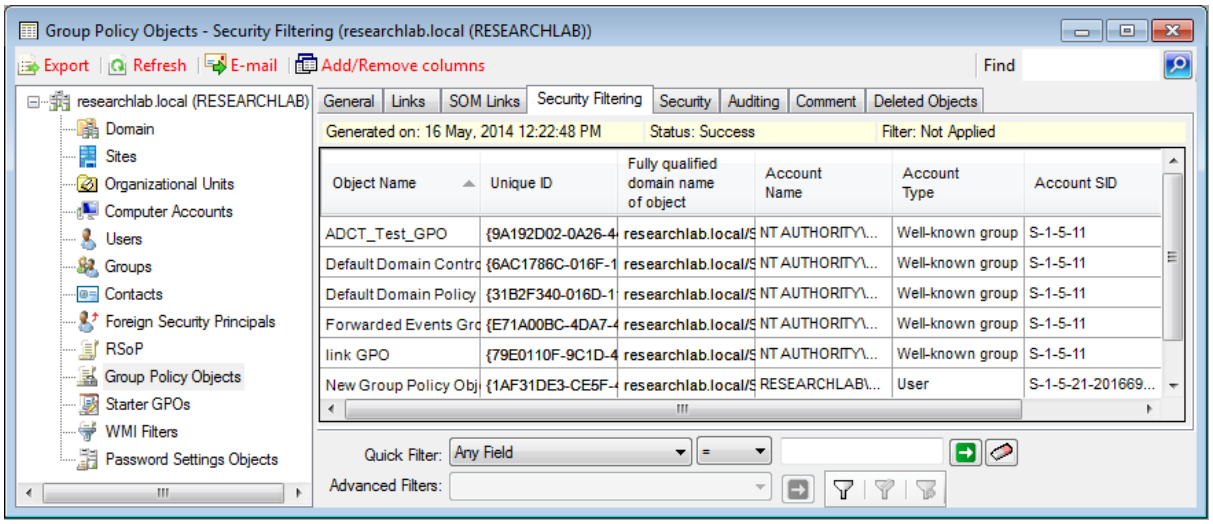
Click on SOM Links tab to view the following information: **{Object Name, Fully qualified domain name of object, Object Type, Block Policy Inheritance, Linked GPO, Linked GPO FQDN, Linked GPO ID, Linked GPO Domain, Link Order, Enforced, Link Enabled}.**

The output would be displayed as shown below:



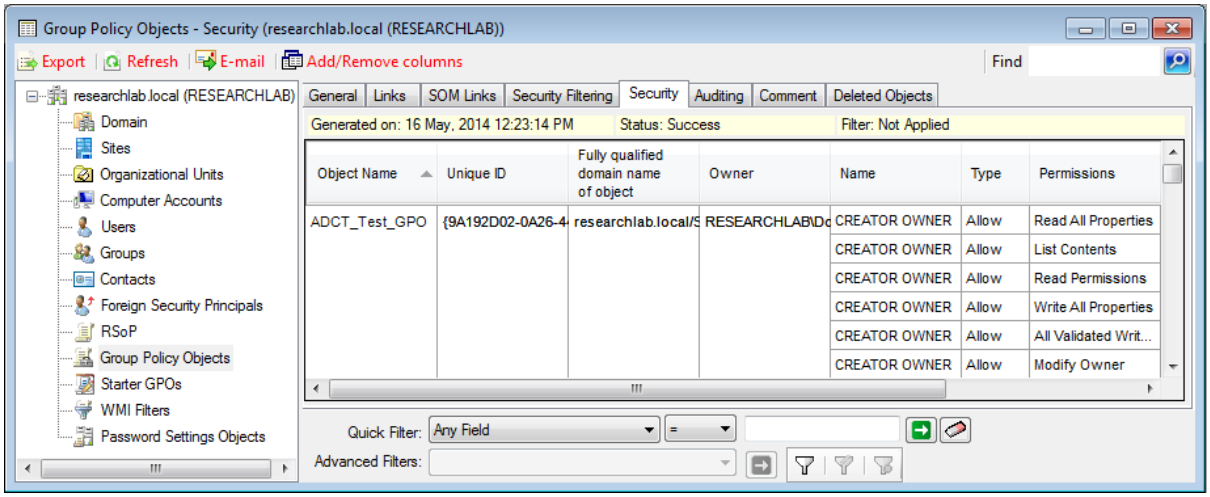
Click on Security Filtering tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Account Name, Account Type, Account SID, Account FQDN**

The output would be displayed as shown below:



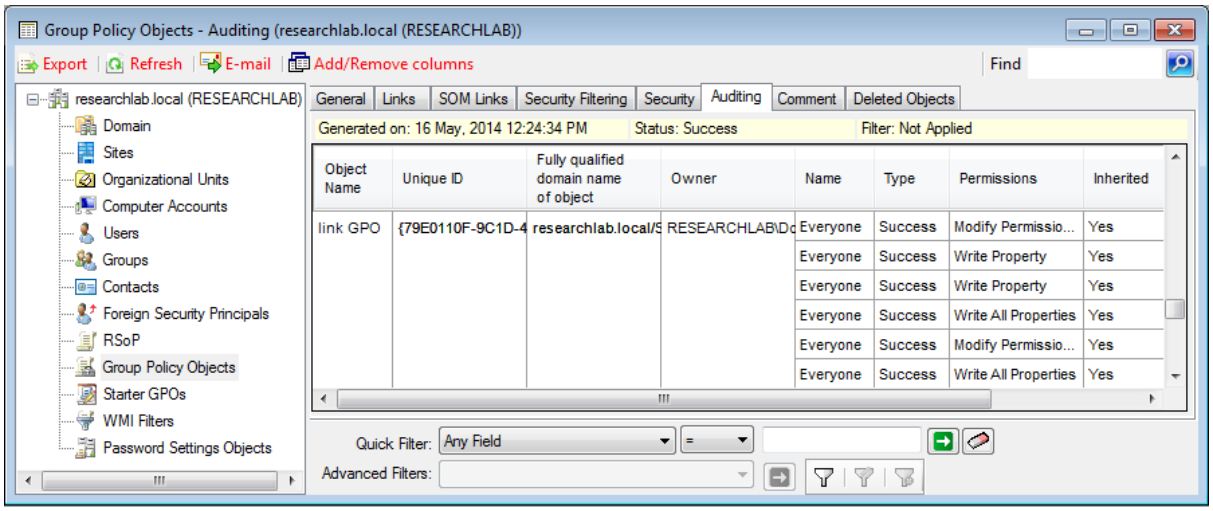
Click on Security tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



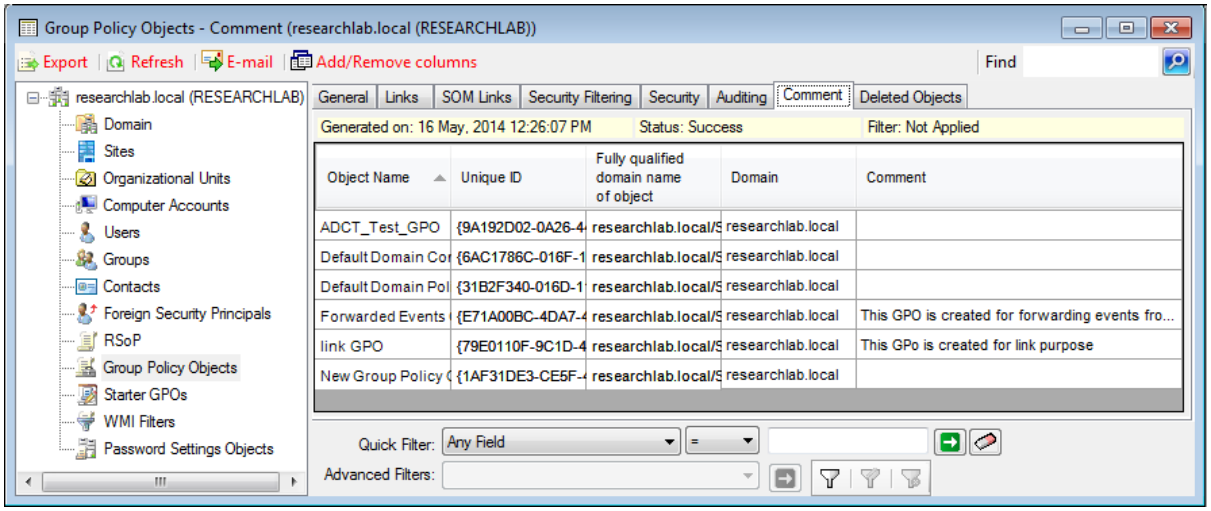
Click on Auditing tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



Click on Comment tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Domain, Comment}.**

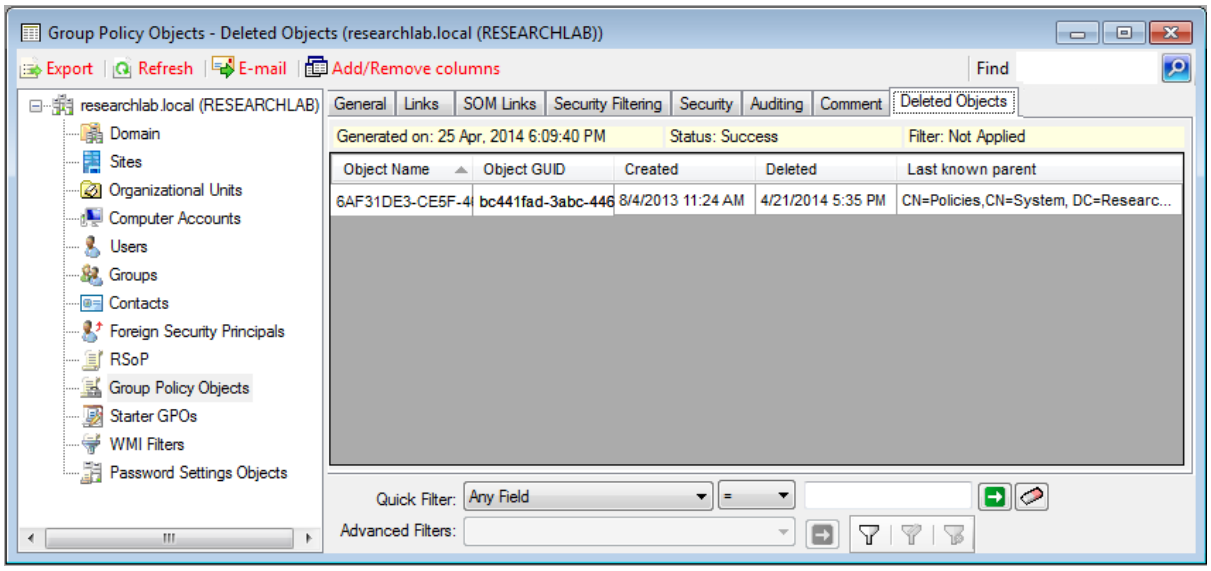
The output would be displayed as shown below:



NOTE: Comment (Win 2008) report is applicable only for ***Windows Server 2008.***

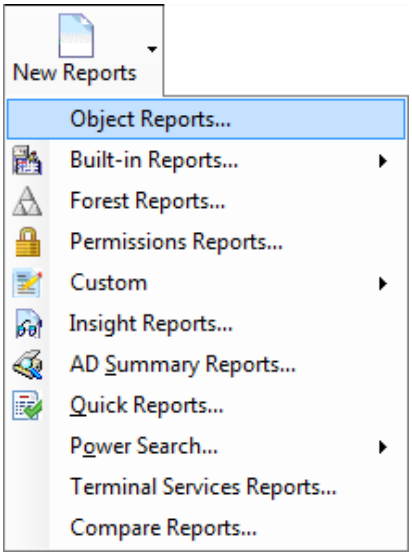
Click on Deleted Objects tab to view the following information: **{Object Name, Object GUID, Created, Deleted, Last known parent}.**

The output would be displayed as shown below:



NOTE: The *"Last known parent"* attribute would be set only on a domain controller running *Windows Server 2003* and later.

3.11 How to view Starter GPOs Reports?



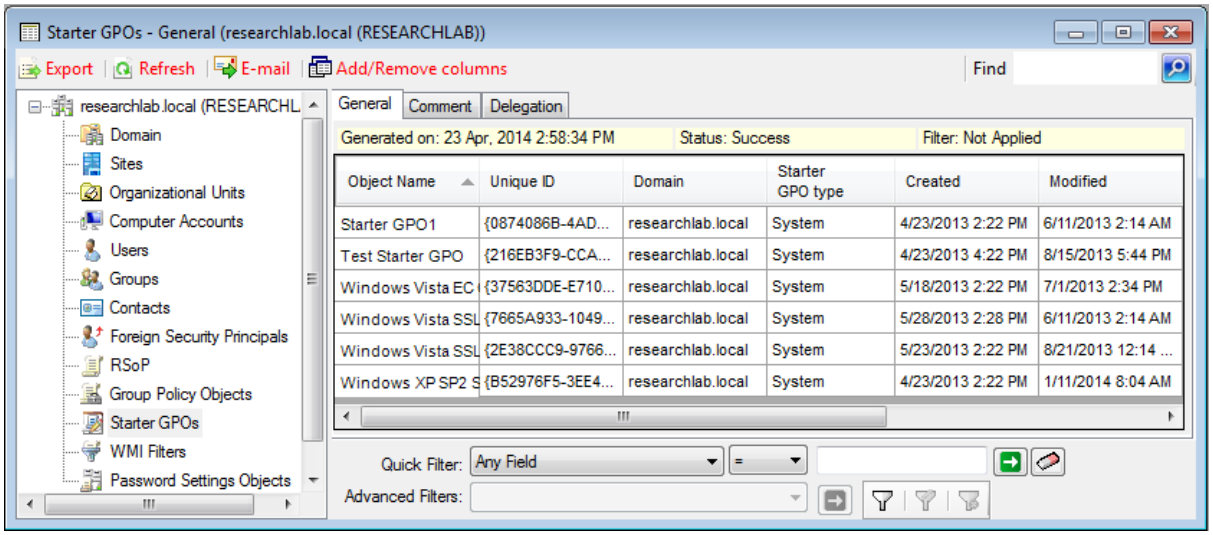
Select *option* under *New Report* button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click **Starter GPOs. *NOTE:*** **Starter GPO reports** require Windows Server 2008 GPMC to be installed on the local computer where ARKAD is running. Also these reports are applicable for Domain Controllers running Windows Server 2008 only.

Click

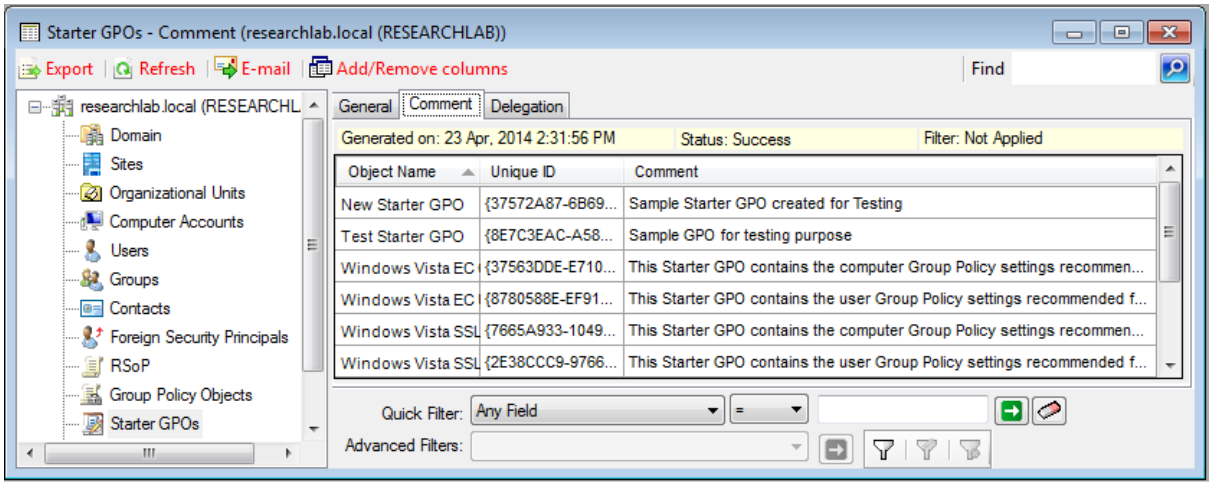
tab to view the following information: **{Object Name, Unique ID, Domain, Starter GPO type, Created, Modified, Version, Author, and Product}.**

The output would be displayed as shown below:



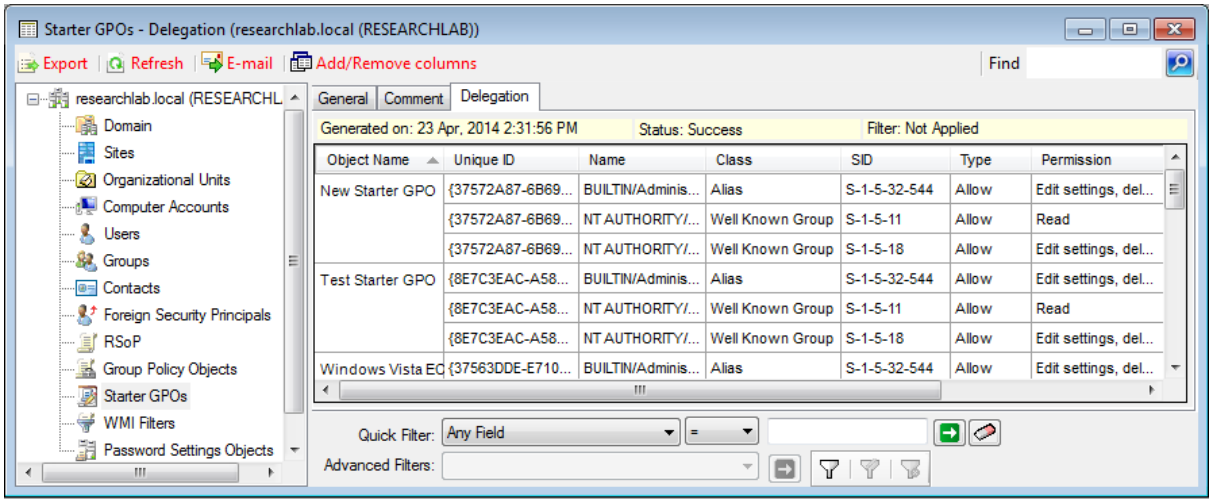
Click on Comment tab to view the following information: **{Object Name, Unique ID, and Comment}.**

The output would be displayed as shown below:

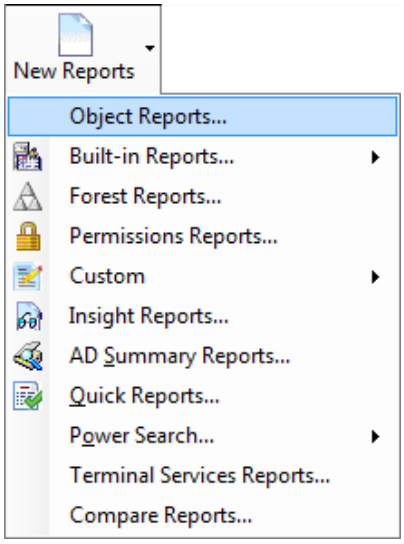


Click on Delegation tab to view the following information: **{Object Name, Unique ID, Name, Class, SID, Type, Permission, Inherited, and Apply To}.**

The output would be displayed as shown below:



3.12 How to view WMI Filter Reports?



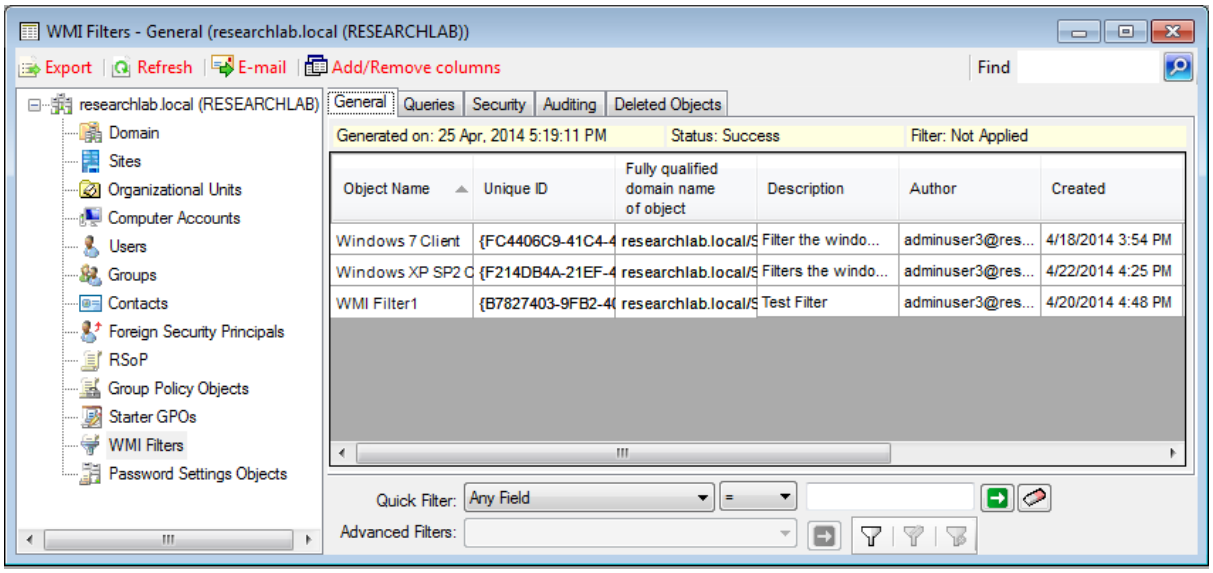
Select *option* under *New Report* button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller*. The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click **WMI Filters.**

Click

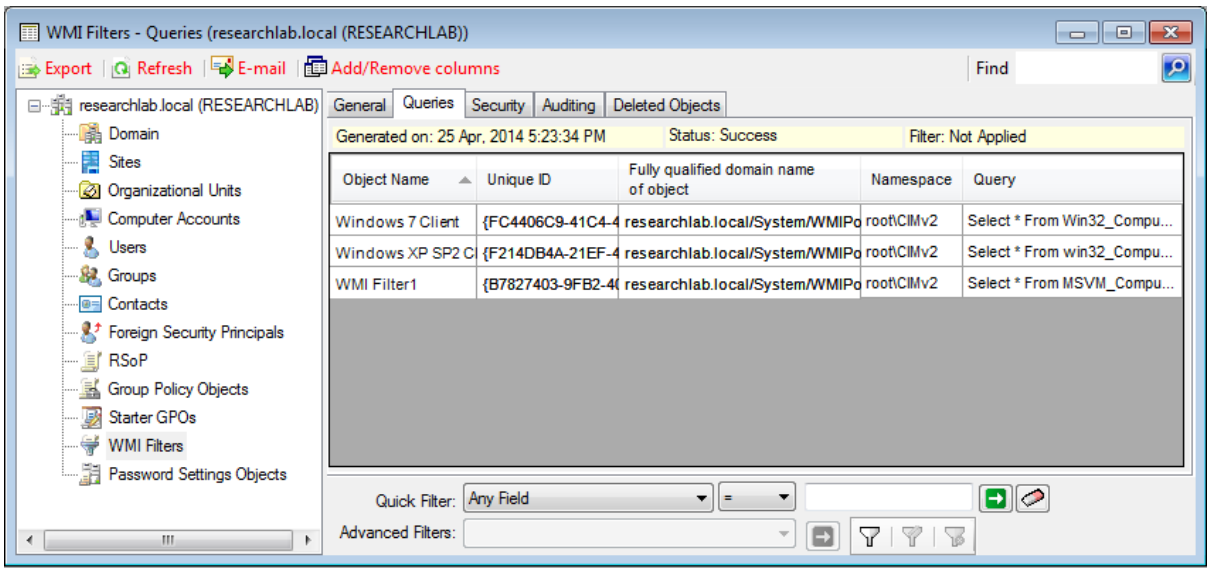
tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Description, Author, Created, Modified, Linked GPO, Linked GPO FQDN}.**

The output would be displayed as shown below:



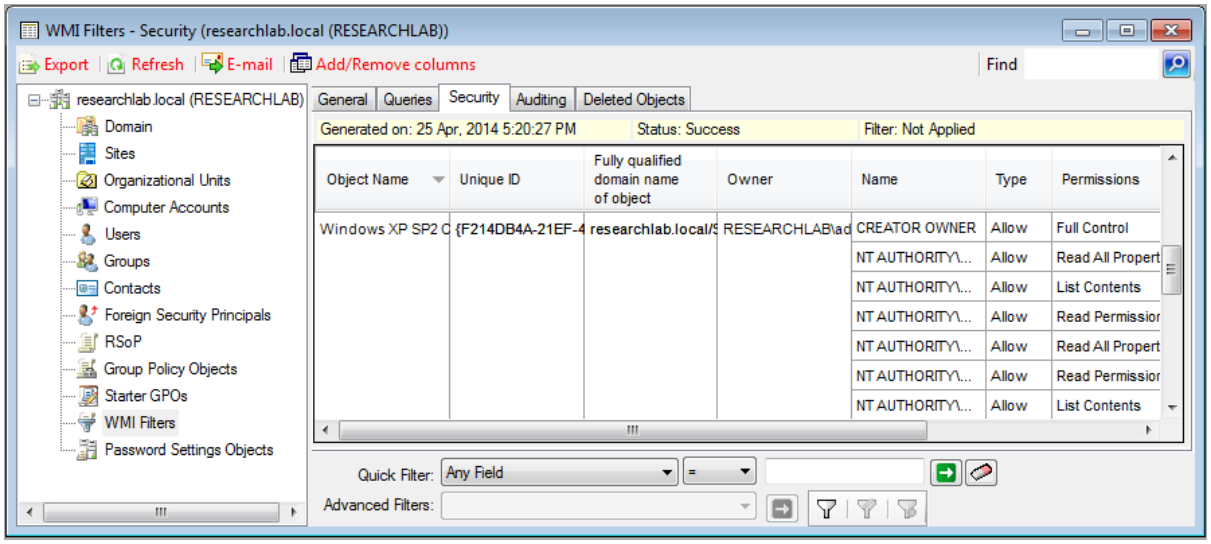
Click on Queries tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Namespace, Query}.**

The output would be displayed as shown below:



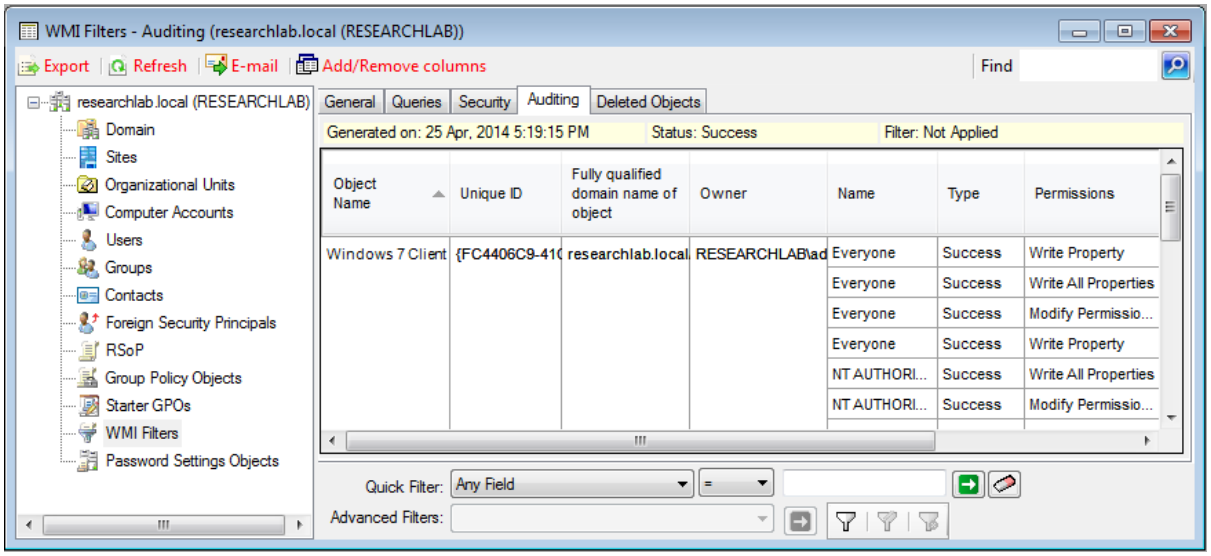
Click on Security tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



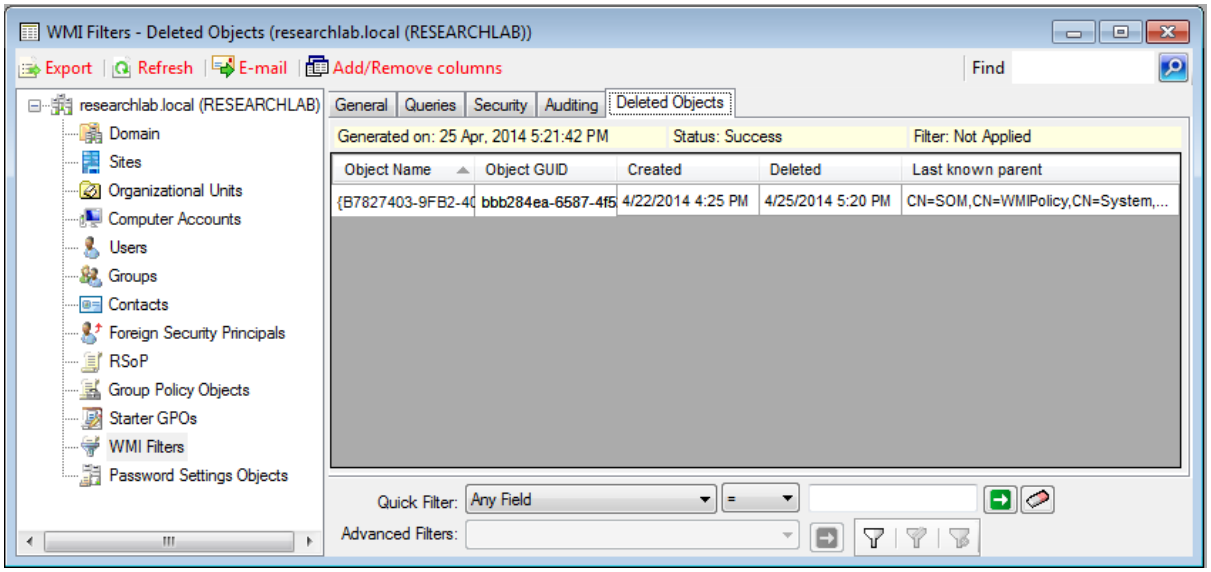
Click on Auditing tab to view the following information: **{Object Name, Unique ID, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



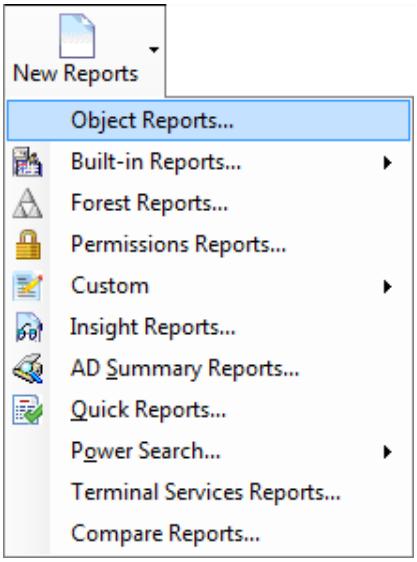
Click Deleted Objects tab to view the following information: **{Object Name, Object GUID, Created, Deleted, Last known parent}.**

The output would be displayed as shown below:



NOTE: The *"Last known parent"* attribute would be set only on a domain controller running *Windows Server 2003* and later.

3.13 How to view Password Settings Objects Reports?



Select *option* under *New Report* button. The Connection Manager will appear on the screen

This will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.

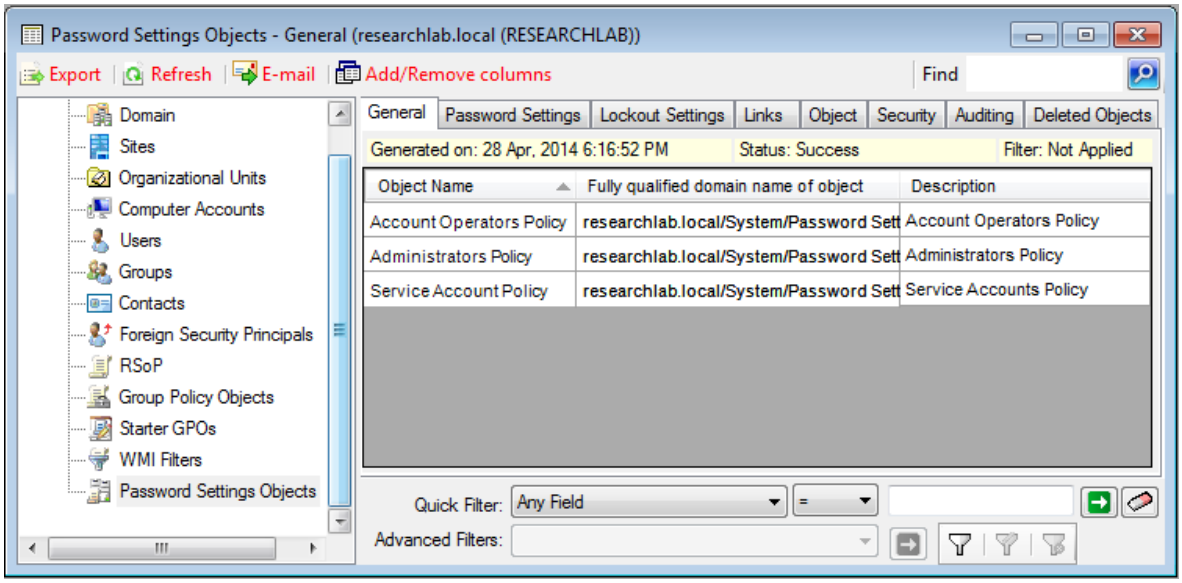
Select and expand the domain node in the left pane of the newly launched report window, and then click **Password Settings Objects.**

NOTE: Password Settings Objects reports are applicable for Domain Controllers running Windows Server 2008 only.

Click

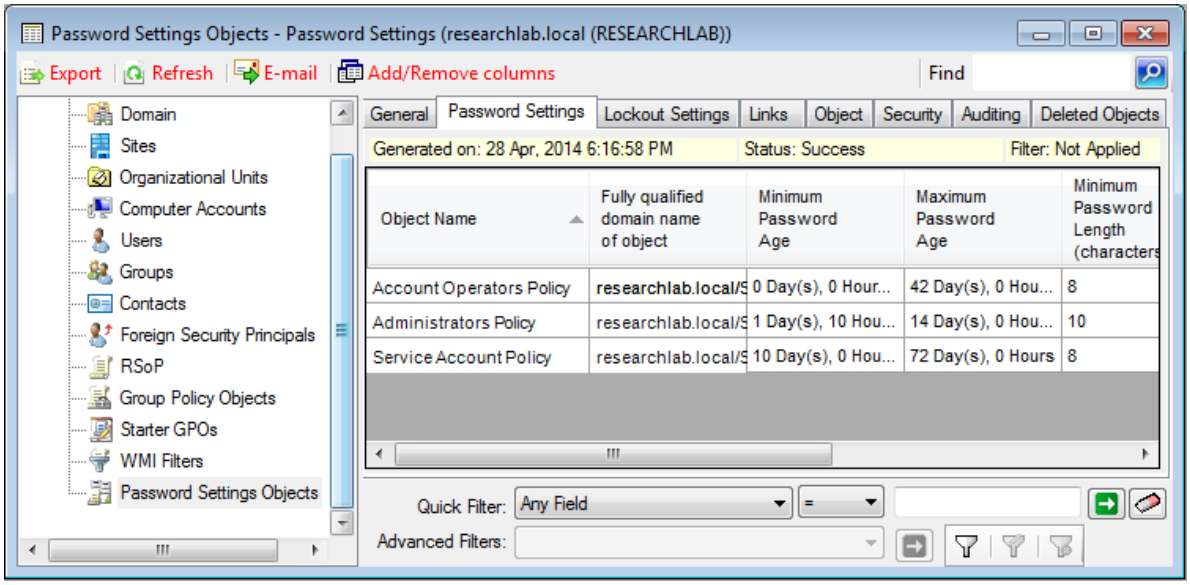
tab to view the following information: **{Object Name, Fully qualified domain name of object, Description}.**

The output would be displayed as shown below:



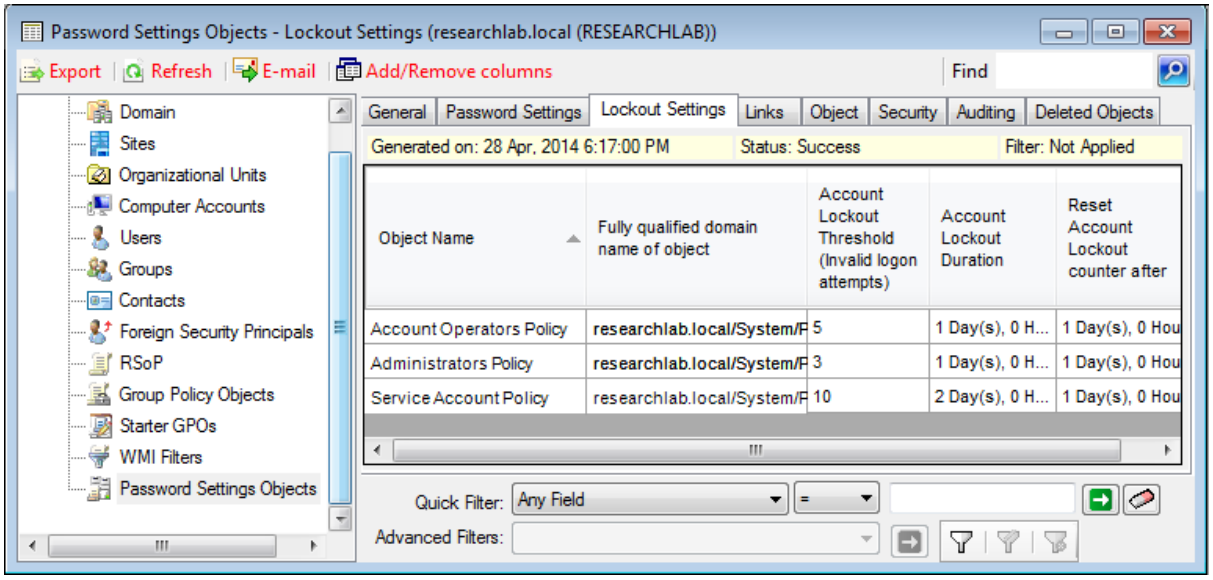
Click on Password Settings tab to view the following information: **{Object Name, Fully qualified domain name of object, Minimum Password Age, Maximum Password Age, Minimum Password Length (characters), Password History Length (Passwords remembered), Password Complexity Enabled, Password Reversible Encryption Enabled}.**

The output would be displayed as shown below:



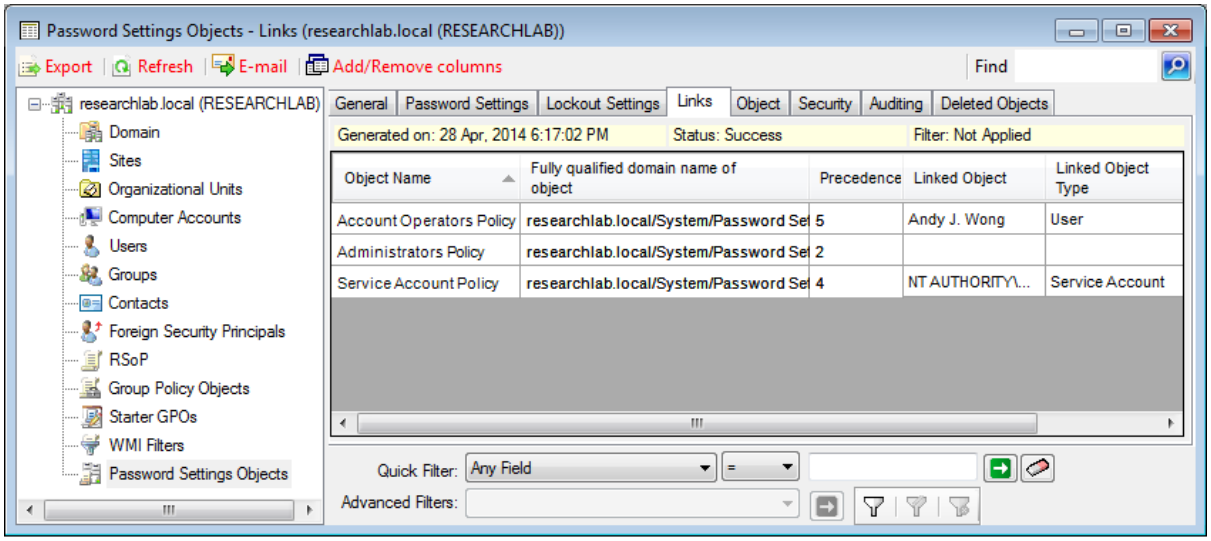
Click on Lockout Settings tab to view the following information: **{Object Name, Fully qualified domain name of object, Account Lockout Threshold (Invalid logon attempts), Account Lockout Duration, Reset Account Lockout counter after}**.

The output would be displayed as shown below:



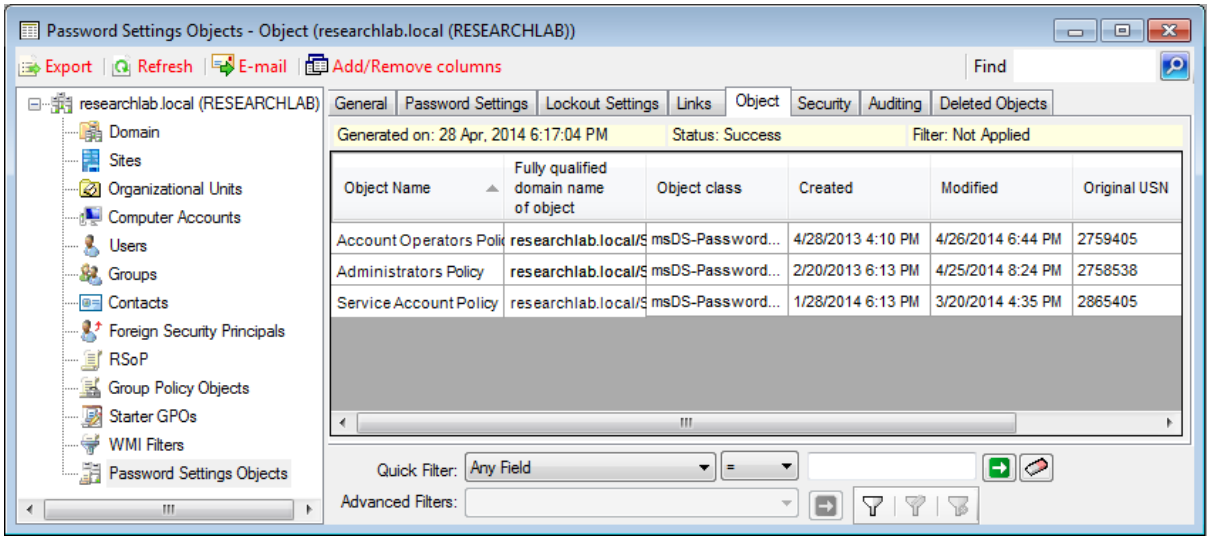
Click on Links tab to view the following information: **{Object Name, Fully qualified domain name of object, Precedence, Linked Object, Linked Object Type, Linked Object FQDN}.**

The output would be displayed as shown below:



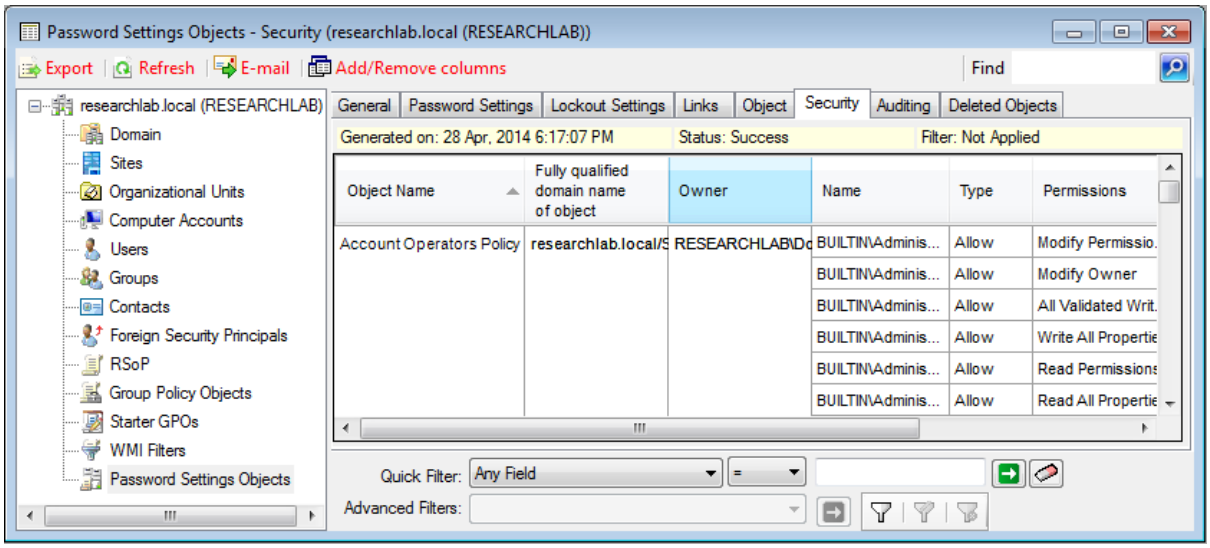
Click on Object tab to view the following information: **{Object Name, Fully qualified domain name of object, Object class, Created, Modified, Original USN, Current USN}.**

The output would be displayed as shown below:



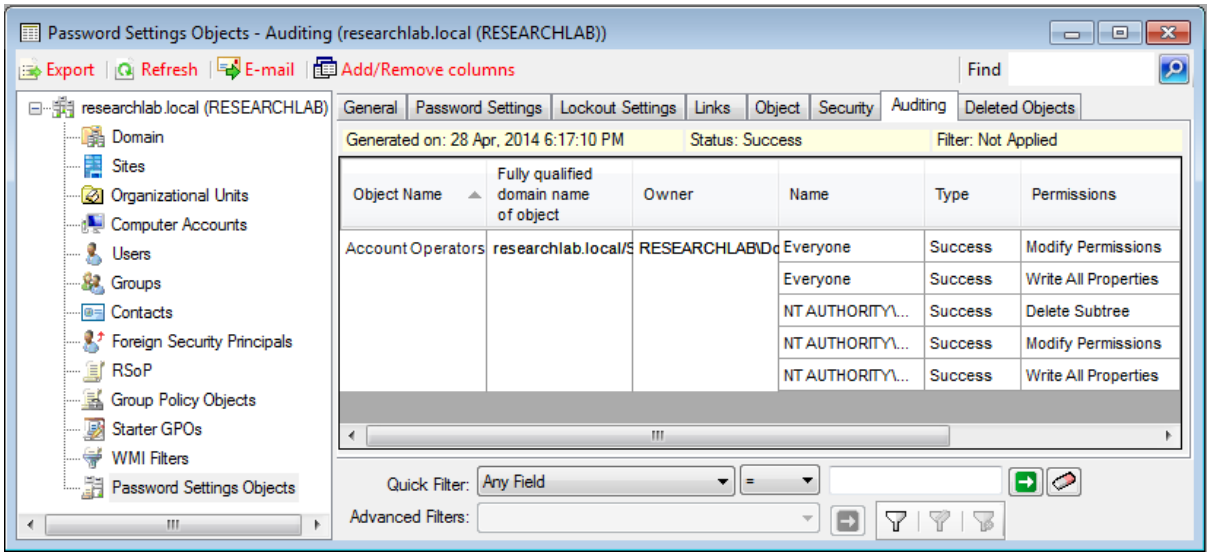
Click on Security tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, and Apply To}.**

The output would be displayed as shown below:



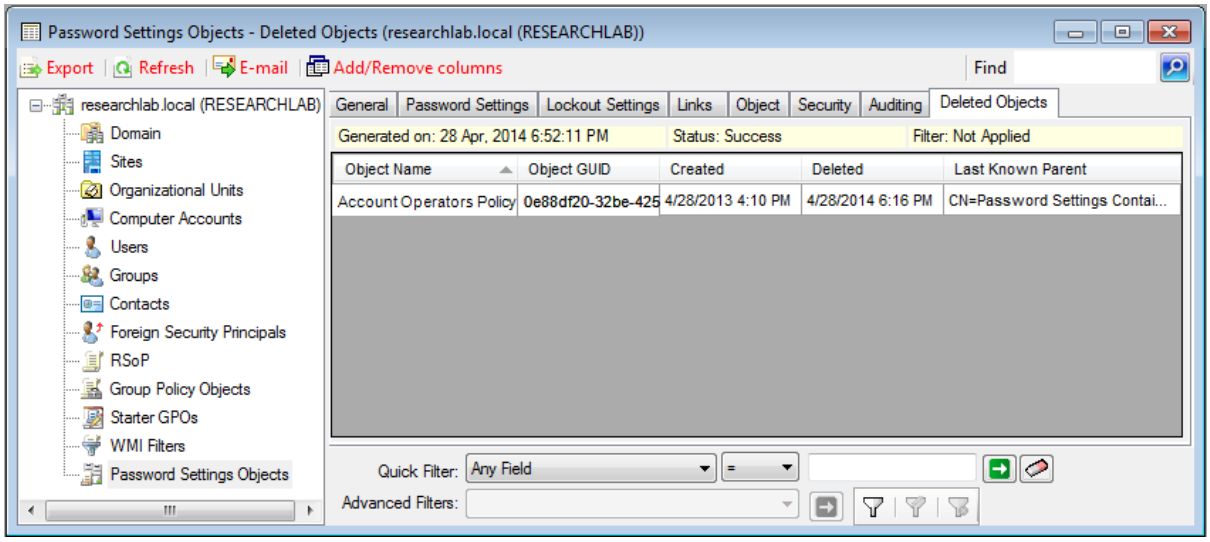
Click on Auditing tab to view the following information: **{Object Name, Fully qualified domain name of object, Owner, Name, Type, Permissions, Inherited, Apply To}.**

The output would be displayed as shown below:



Click on tab to view the following information: **{Object Name, Object GUID, Created, Deleted, Last known parent}.**

The output would be displayed as shown below:



NOTE: The *"Last known parent"* attribute would be set only on a domain controller running *Windows Server 2003* and later.

Chapter 4

4 Quick Reports

4.1 About Quick Reports

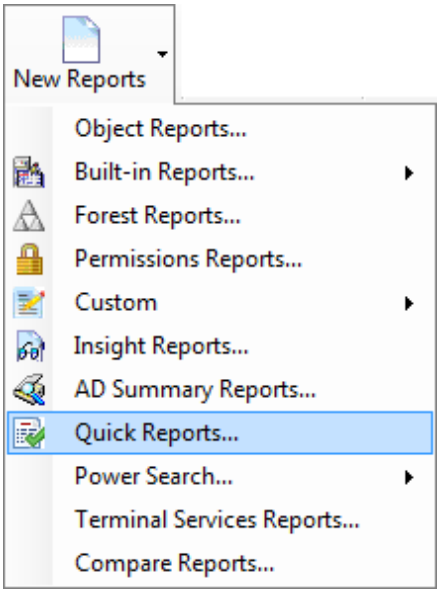
The ***Quick Reports*** feature in ARKAD provides a quick and consistent way for administrators to retrieve specific information from an *Active Directory Domain.*

Currently, the Quick Reports feature includes reports of Groups, Users, Contacts and Computer Accounts.

The benefits of using the Quick Reports are as follows:

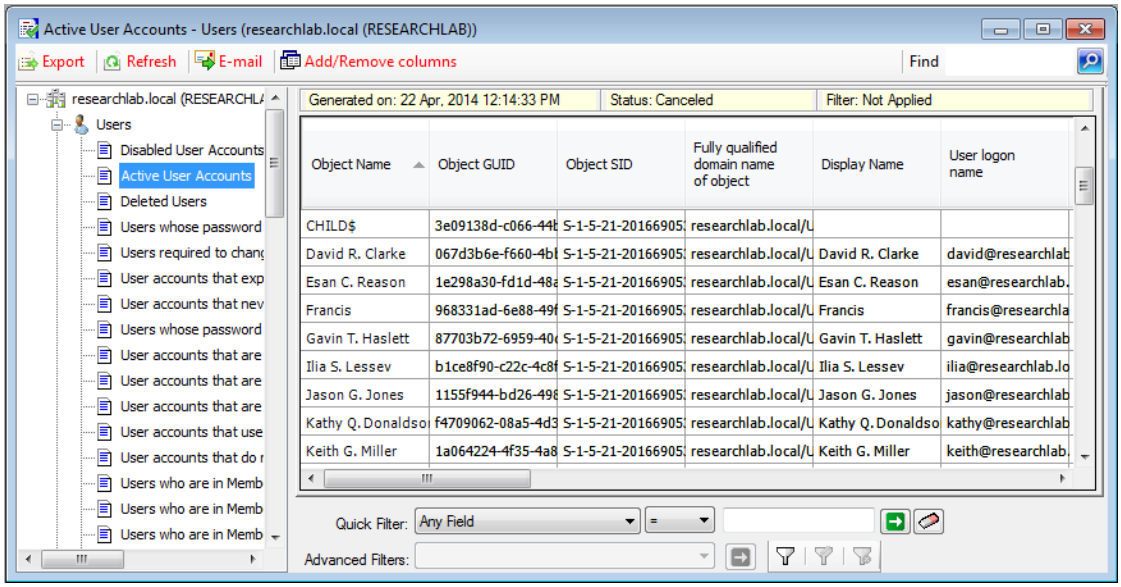
1) *Reports* can be generated for particular information at Active Directory.
2) *Export and E-mail* the generated reports.

4.2 How to generate Quick Reports?



Select *option* under *New Report* button. The *Connection Manager* will appear on the screen which will allow you to *select* a *domain* and a corresponding *domain controller.* The report window will be launched after the domain and the selected domain controller are validated.

This window shows the list of reports that can be generated. Select a report from the list of reports under domain node. After the data collection process is complete, the report would be generated in a report window as shown below:


Active User Accounts - Users (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Add/Remove columns
Find
researchlab.local (RESEARCHLA
Users
Disabled User Accounts
Active User Accounts
Deleted Users
Users whose password
Users required to chang
User accounts that exp
User accounts that nev
Users whose password
User accounts that are
User accounts that are
User accounts that are
User accounts that use
User accounts that do
Users who are in Memb
Users who are in Memb
Users who are in Memb
Generated on: 22 Apr, 2014 12:14:33 PM
Status: Canceled
Filter: Not Applied
Object Name
Object GUID
Object SID
Fully qualified domain name of object
Display Name
User logon name
CHILD$ 3e09138d-c066-44 S-1-5-21-20166905 researchlab.local/U
David R. Clarke 067d3b6e-f660-4b S-1-5-21-20166905 researchlab.local/U David R. Clarke david@researchlab
Esan C. Reason 1e298a30-fd1d-48 S-1-5-21-20166905 researchlab.local/U Esan C. Reason esan@researchlab.
Francis 968331ad-6e88-49 S-1-5-21-20166905 researchlab.local/U Francis francis@researchla
Gavin T. Haslett 87703b72-6959-40 S-1-5-21-20166905 researchlab.local/U Gavin T. Haslett gavin@researchlab
Ilia S. Lessev b1ce8f90-c22c-4c8 S-1-5-21-20166905 researchlab.local/U Ilia S. Lessev ilia@researchlab.lo
Jason G. Jones 1155f944-bd26-49 S-1-5-21-20166905 researchlab.local/U Jason G. Jones jason@researchlab
Kathy Q. Donaldso f4709062-08a5-4d3 S-1-5-21-20166905 researchlab.local/U Kathy Q. Donaldso kathy@researchlab
Keith G. Miller 1a064224-4f35-4a8 S-1-5-21-20166905 researchlab.local/U Keith G. Miller keith@researchlab.
Quick Filter:
Any Field
Advanced Filters:

Chapter 5

5 Built-in Reports

5.1 About Built-in Reports

The ***Built-in reports*** feature provides several reports to retrieve frequently accessed information across *Active Directory*. Built-in reports are easy to use and speeds-up the report generation process.

The built-in reports feature provides reports on the following resource categories.

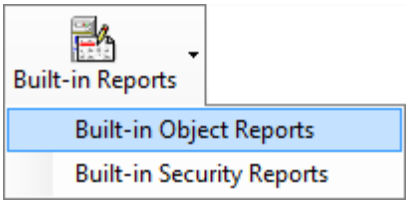
- Built-in *Object Reports*
- Built-in *Security Reports*

The benefits of using the Built-in reports are as follows:

1) Easy to *view* frequently accessed significant information. Ex: Recently Created / Modified / Deleted objects report.
2) *Reports* can be generated for particular information at Active Directory.
3) *Modify* the Parameters of the several reports.
4) *Export* and *Email* the generated reports.

5.2 How to Generate Built-in Object Reports?

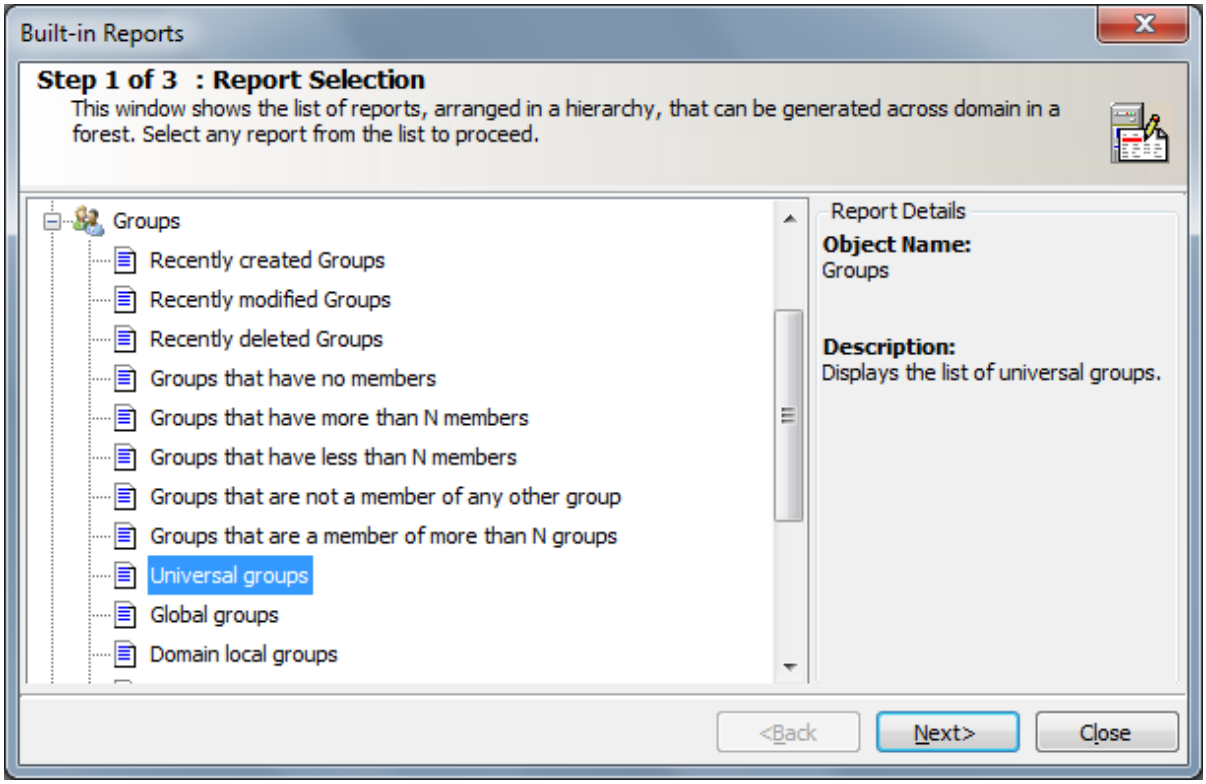
Perform the following steps to generate a ***Built-in object report.***

Select 

under Built-in Reports button in the tool bar.

Step 1: Report Selection

1) The *Built-in Reports* window with the list of reports will be displayed as shown below:

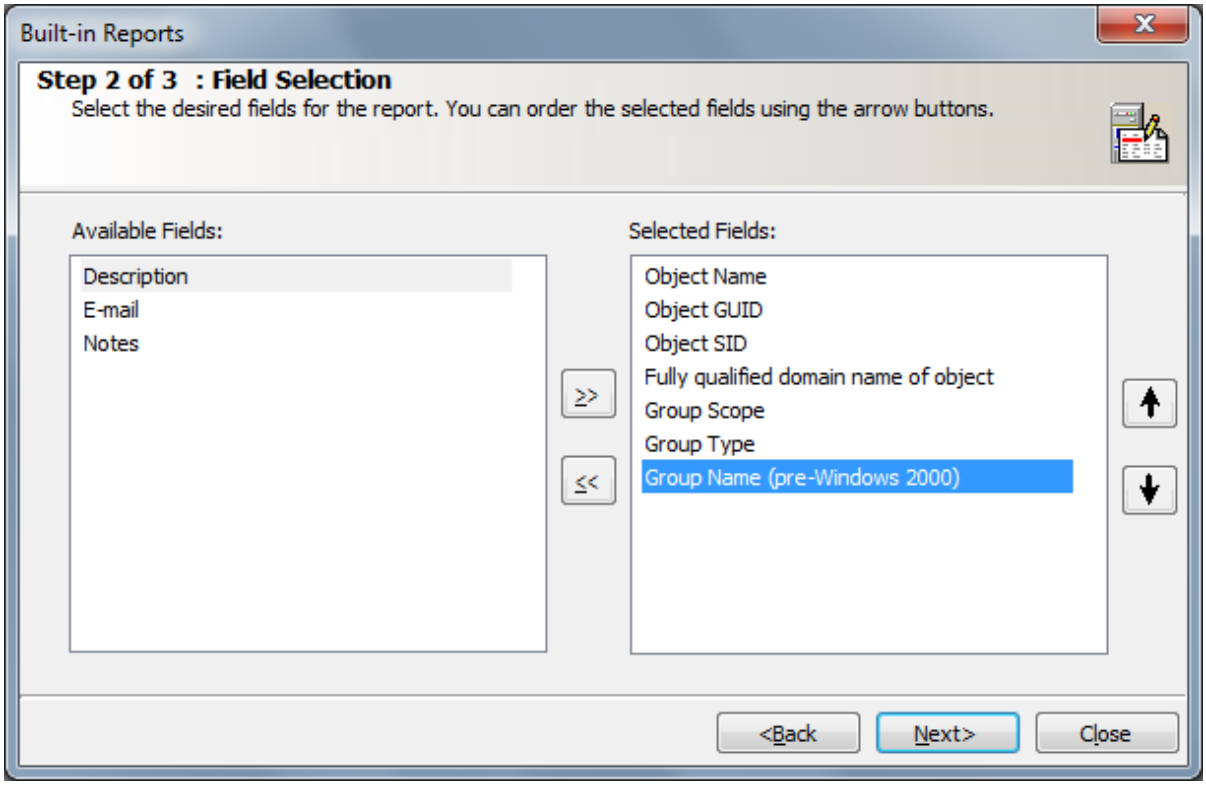

Built-in Reports
Step 1 of 3 : Report Selection
This window shows the list of reports, arranged in a hierarchy, that can be generated across domain in a forest. Select any report from the list to proceed.
Groups
Recently created Groups
Recently modified Groups
Recently deleted Groups
Groups that have no members
Groups that have more than N members
Groups that have less than N members
Groups that are not a member of any other group
Groups that are a member of more than N groups
Universal groups
Global groups
Domain local groups
Report Details
Object Name:
Groups
Description:
Displays the list of universal groups.
<Back
Next>
Close

2) This window shows the *list of reports* that can be generated across domain/domains in a forest. *Select* a report from the *list of reports.*

Click ***Next*** to proceed to the next step.

Step 2: Field Selection

1) To select *fields* from a report, click on the *desired field* in the list of *Available Fields,* and then *click* *button.*



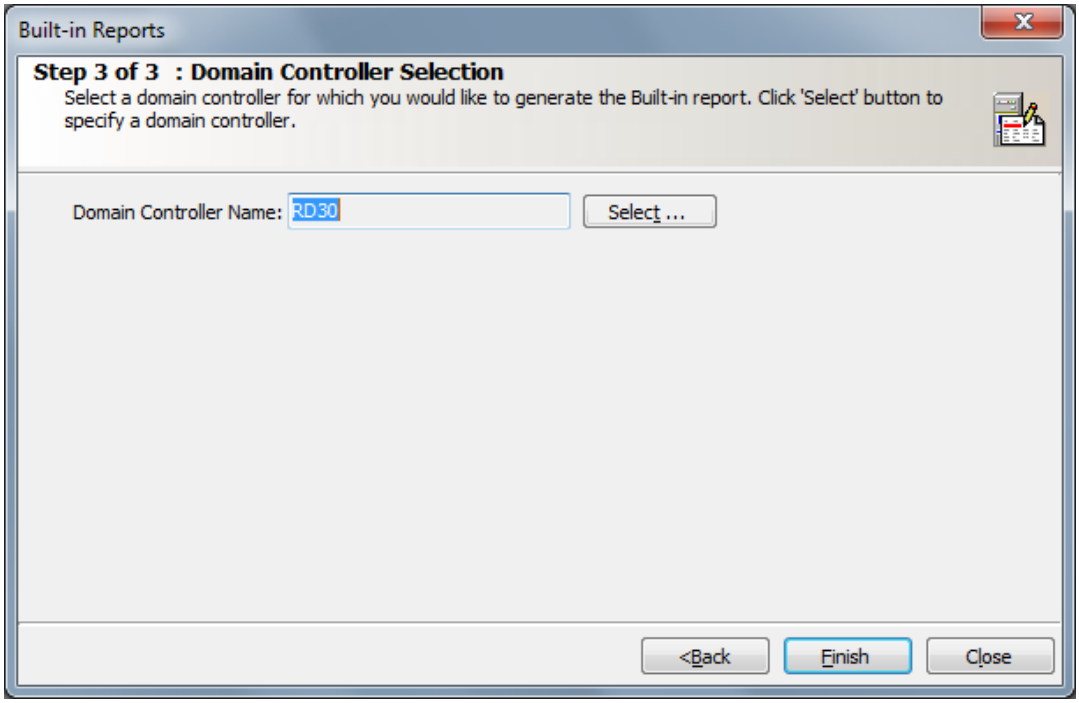
2) To *remove selected fields*, click on the desired field in the list of Selected Fields, and then *click* *button.*

3) You can use the *arrow buttons* to order the selected fields. To move a *field up* by one position in the list of selected fields *click* *button.* To move a *field down* by one position in the list of selected fields *click* *button.*

4) Click ***Next*** to proceed to the next Step.

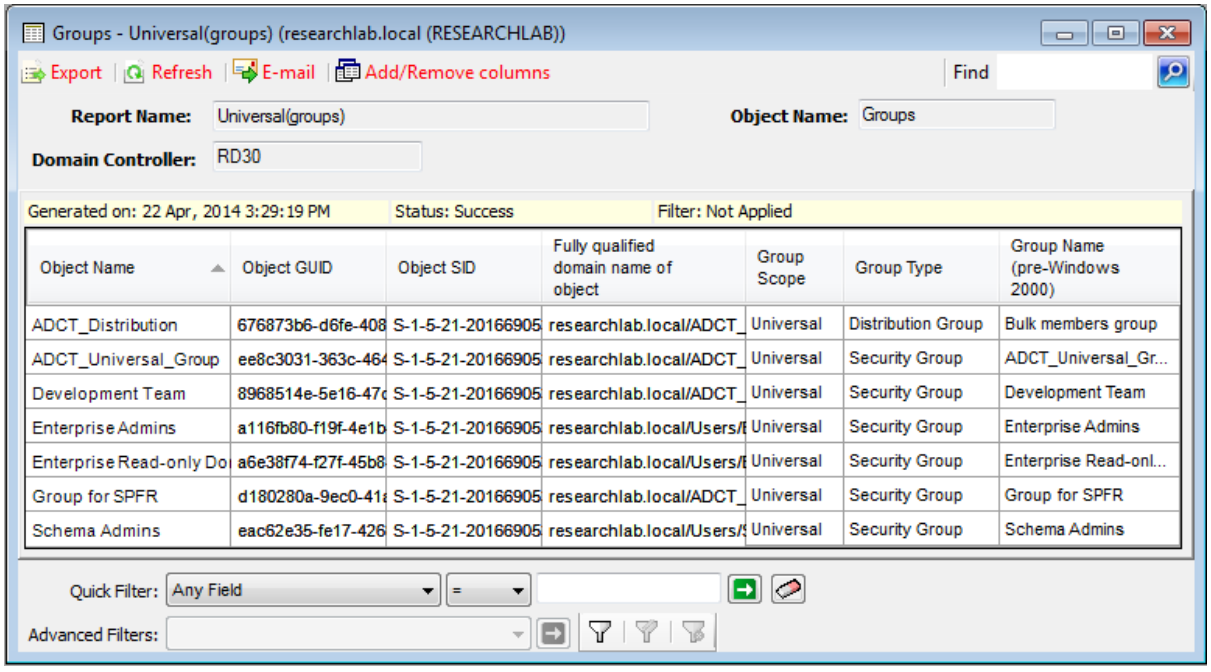
Step 3: Server Selection

1) Specify a *domain controller* for which you want to generate the selected Built-in report. Click ***Select*** button to specify a *domain controller*. The Connection Manager will be displayed which will allow you to specify a domain controller.


Built-in Reports
Step 3 of 3 : Domain Controller Selection
Select a domain controller for which you would like to generate the Built-in report. Click 'Select' button to specify a domain controller.
Domain Controller Name:
RD30
Select ...
<Back
Finish
Close

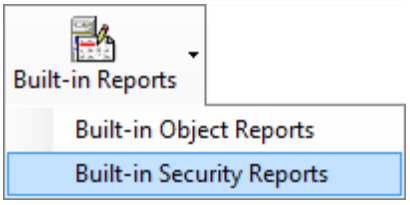
2) Click ***Finish*** to generate the report.

After the data collection process is complete, the report would be generated in a report window as shown below:



5.3 How to Generate Built-in Security Reports?

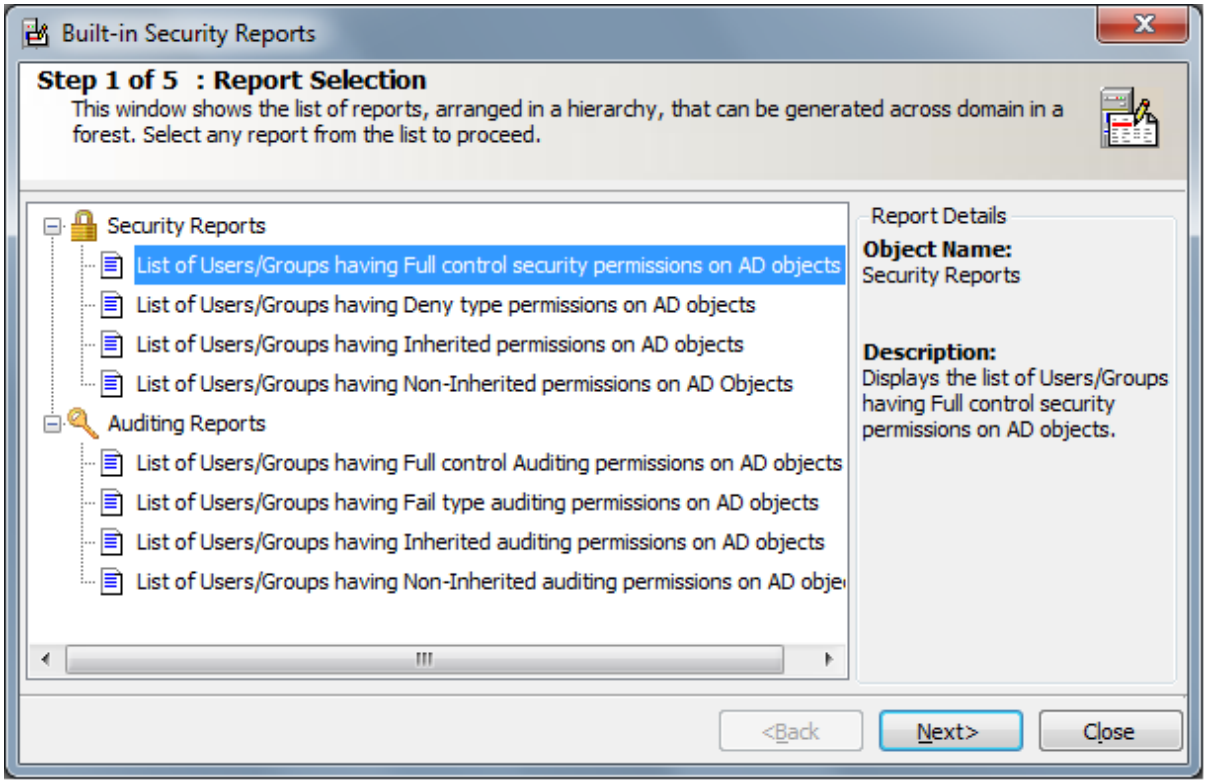
Perform the following steps to generate a **Built-in Security report.**

Select 

under *Built-in Reports* button in the tool bar.

Step 1: Report Selection

1) The *Built-in Reports* window with the *list of reports* will be displayed as shown below:

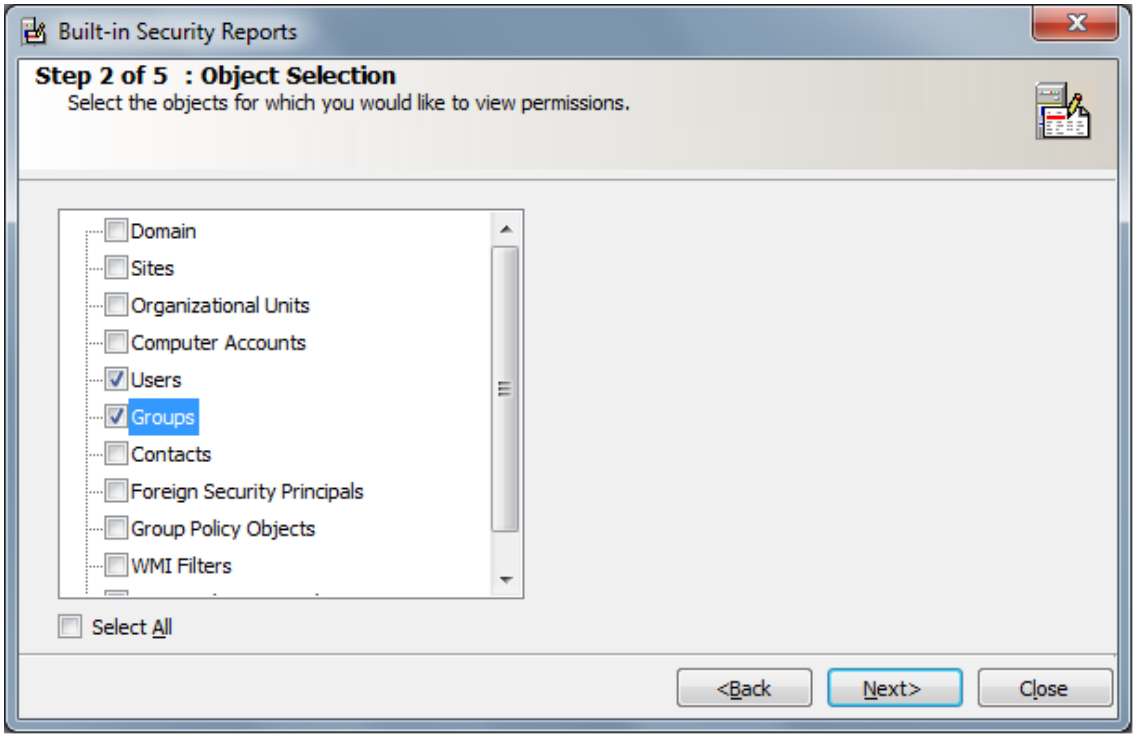

Built-in Security Reports
Step 1 of 5 : Report Selection
This window shows the list of reports, arranged in a hierarchy, that can be generated across domain in a forest. Select any report from the list to proceed.
Security Reports
List of Users/Groups having Full control security permissions on AD objects
List of Users/Groups having Deny type permissions on AD objects
List of Users/Groups having Inherited permissions on AD objects
List of Users/Groups having Non-Inherited permissions on AD Objects
Auditing Reports
List of Users/Groups having Full control Auditing permissions on AD objects
List of Users/Groups having Fail type auditing permissions on AD objects
List of Users/Groups having Inherited auditing permissions on AD objects
List of Users/Groups having Non-Inherited auditing permissions on AD obje
Report Details
Object Name:
Security Reports
Description:
Displays the list of Users/Groups having Full control security permissions on AD objects.
<Back
Next>
Close

2) This window shows the list of reports that can be generated across domain/domains in a forest. Select a report from the list of reports.

Click ***Next*** to proceed to the next step.

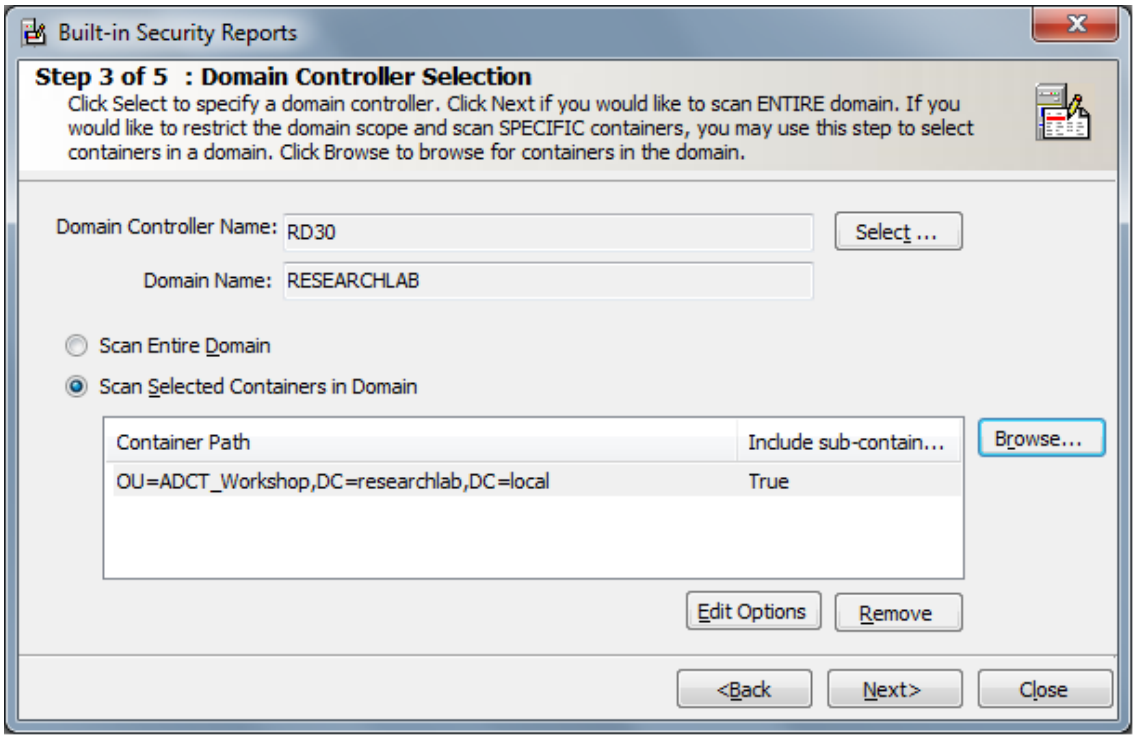
Step 2: Object Selection

1) *Select* the desired **object**(s) from the list, using the **checkboxes,** for which you want to view **permissions** defined.

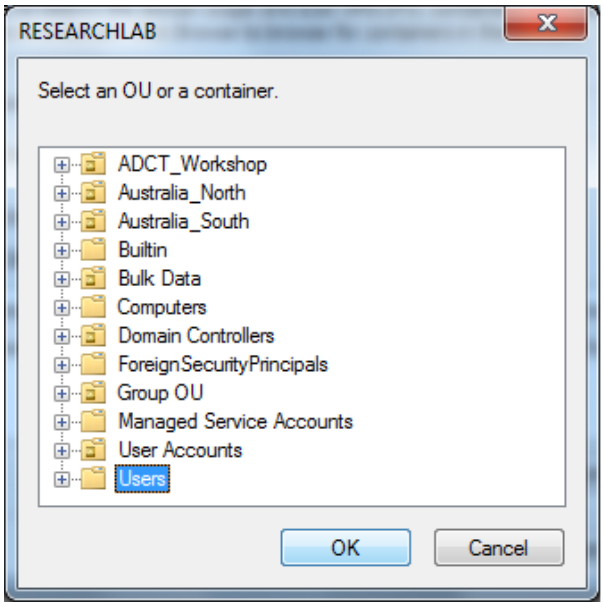


2) Click ***Next*** to proceed to the next step.

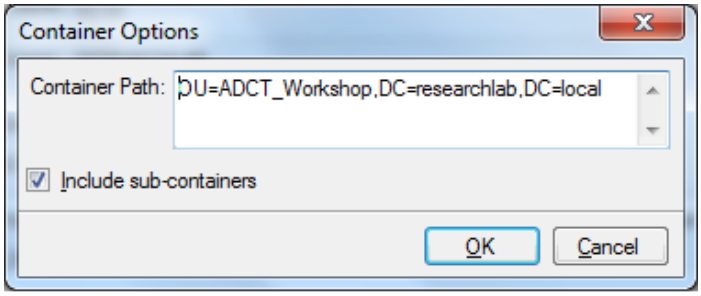
Step 3: Domain Controller Selection


Built-in Security Reports
Step 3 of 5 : Domain Controller Selection
Click Select to specify a domain controller. Click Next if you would like to scan ENTIRE domain. If you would like to restrict the domain scope and scan SPECIFIC containers, you may use this step to select containers in a domain. Click Browse to browse for containers in the domain.
Domain Controller Name: RD30
Select ...
Domain Name: RESEARCHLAB
Scan Entire Domain
Scan Selected Containers in Domain
Container Path
Include sub-contain...
OU=ADCT_Workshop,DC=researchlab,DC=local
True
Browse...
Edit Options
Remove
<Back
Next>
Close

1) Click S**elect** to specify a *domain controller* and corresponding domain for which you want the report generated. The *Connection Manager* will be displayed which will allow you to specify a domain controller. Note that the report can be generated only against the domain you specify in this step. During report generation you may specify any domain controller that belongs to the selected domain.
2) You may *select* specific containers in the domain to restrict the domain scope and collect data for objects in selected containers. If no containers are selected, data will be collected by searching the entire domain structure.
3) In order to select specific containers, select **Scan Selected Containers in Domain** option, and then click **Browse** to select containers in the domain. The **container browser** dialog will be displayed as shown below:

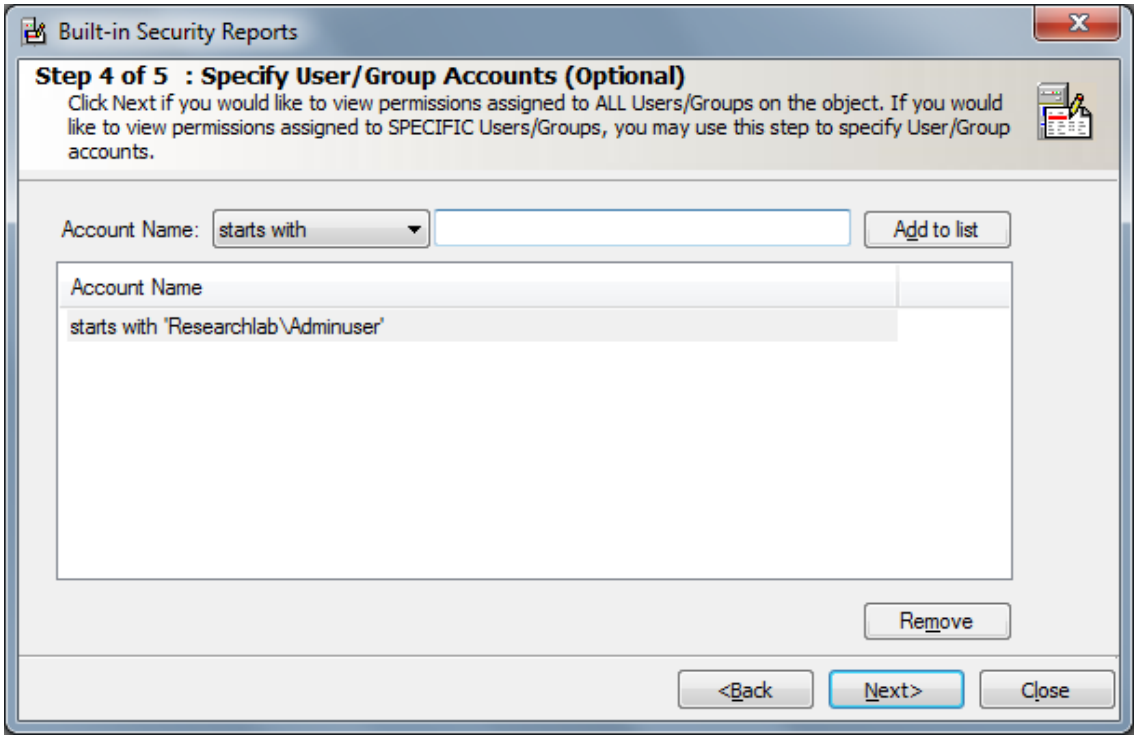


4) ***Select*** the desired container and click **OK.** Note that only one container may be selected at a time. To select another container, click **Add From.** Note that ARKAD scans the specified container for the objects selected in Step 2 of this wizard
5) ARKAD defaults to scanning all the sub-containers under a given container. If you want to change the Include sub-containers option click **Edit Options.** The **Container Options** dialog will be displayed as shown below:



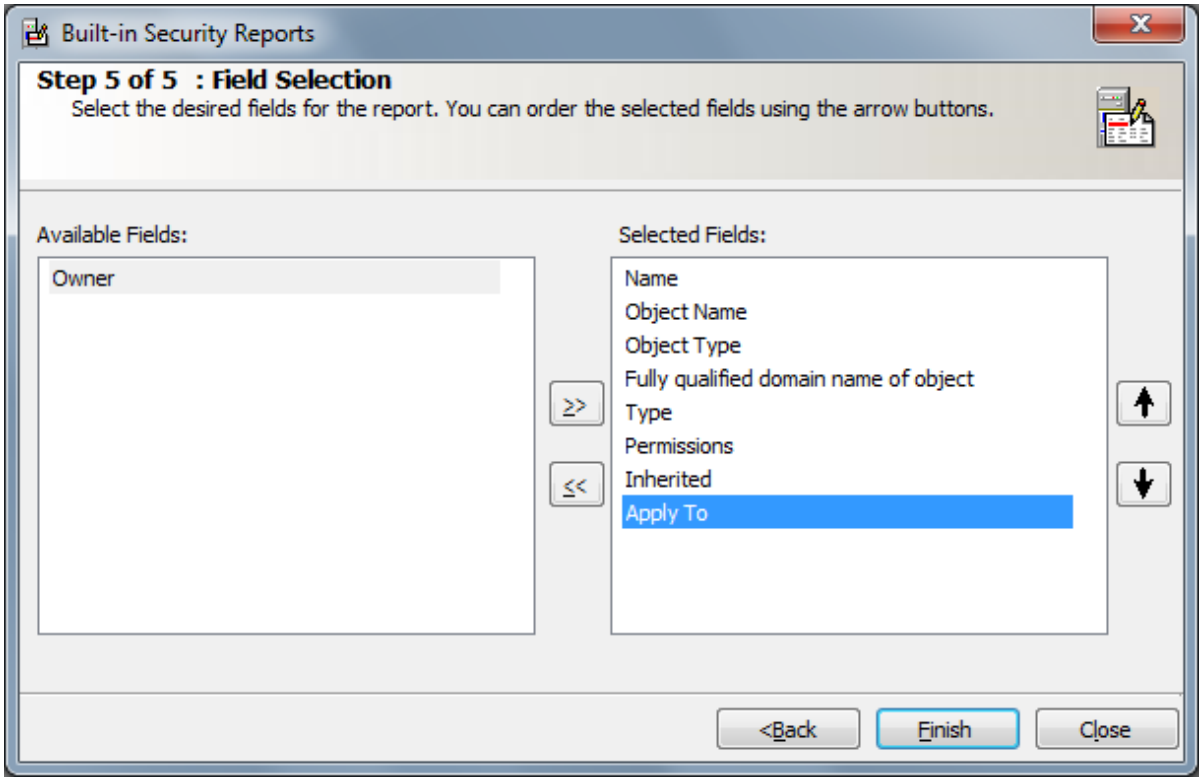
6) Please note that Container Selection is not applicable for Domain, Sites, GPOs and WMI Filters.
7) Click ***Next*** to proceed to the next step.

Step 4: Specify User/Group Accounts (Optional)


Built-in Security Reports
Step 4 of 5 : Specify User/Group Accounts (Optional)
Click Next if you would like to view permissions assigned to ALL Users/Groups on the object. If you would like to view permissions assigned to SPECIFIC Users/Groups, you may use this step to specify User/Group accounts.
Account Name:
starts with
Add to list
Account Name
starts with 'Researchlab\Adminuser'
Remove
<Back
Next>
Close

1) ***Specify user and/or group account*** names to view permissions assigned to specific accounts on objects in the directory.
2) ***Select*** an *operator* from the drop-down list, and then specify an account name to add to the list. You may specify a part of account name to include in list by using operators other than equals (=) and not equals (<>). Note that for equals and not equals operators you have to specify account name in *"Domain Name\Account Name"* format.
3) Click ***Add to list*** to add the specified account name to list.
4) Click ***Next*** to proceed to the next step.

Step 5: Field Selection



1) To **select fields** for the report, click on the desired field in the list of **Available Fields**, and then *click* *button.*

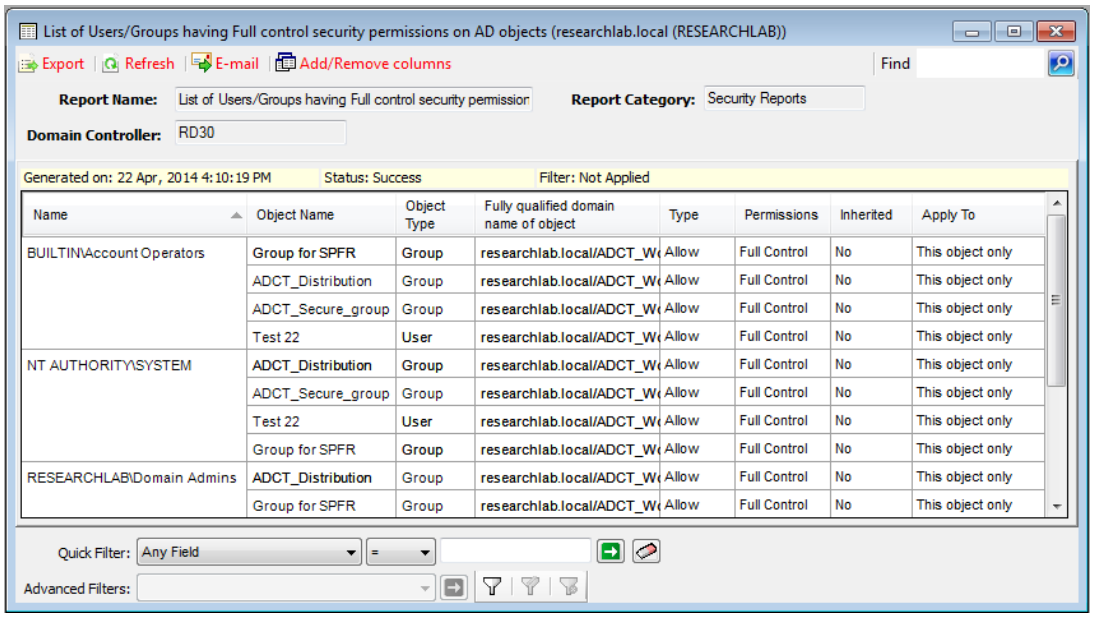
2) To **remove** selected fields, click on the desired field in the list of **Selected Fields**, and then *click* *button.*

3) You can use the **arrow** buttons to order the selected fields. To move a *field up* by one position in the list of selected fields *click* *button.* To move a *field down* by one position in the list of selected fields *click* *button.*

4) Click ***Finish*** to save the permissions report.

CHAPTER 5–Built-in Reports

After the data collection process is complete, the report would be generated in a report window as shown below:



Chapter 6

6 Forest Reports

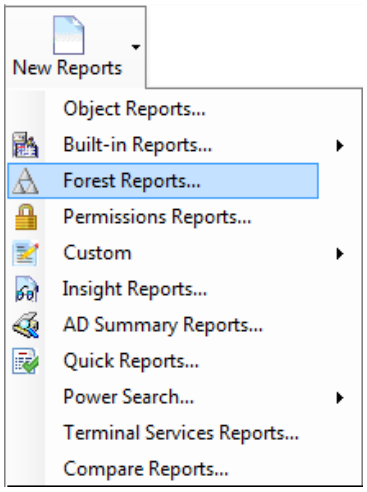
6.1 About Forest Reports

The *Forest Reports* feature in ARKAD allows the user to generate reports across domains in a forest. Also, forest reports can be scheduled for off-line generation by using the Power Export Tool. In ARKAD, forest reports can be generated across domains by specifying a Global Catalog server.

Currently, the *Forest Reports* feature includes reports of Domain, Sites, Groups, Users, Contacts and Group Policy Objects (under Object Reports category) that can be generated across domains in a forest.

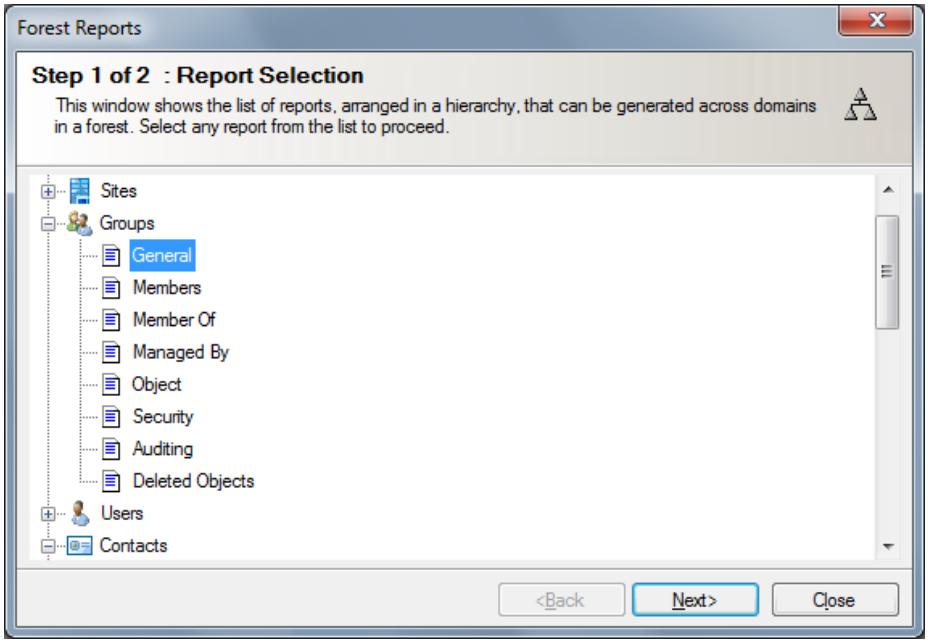
6.2 How to generate Forest Reports?

Perform the following steps to generate a **forest report**.

1) ***Select*** 

under *New Report* button in the tool bar.

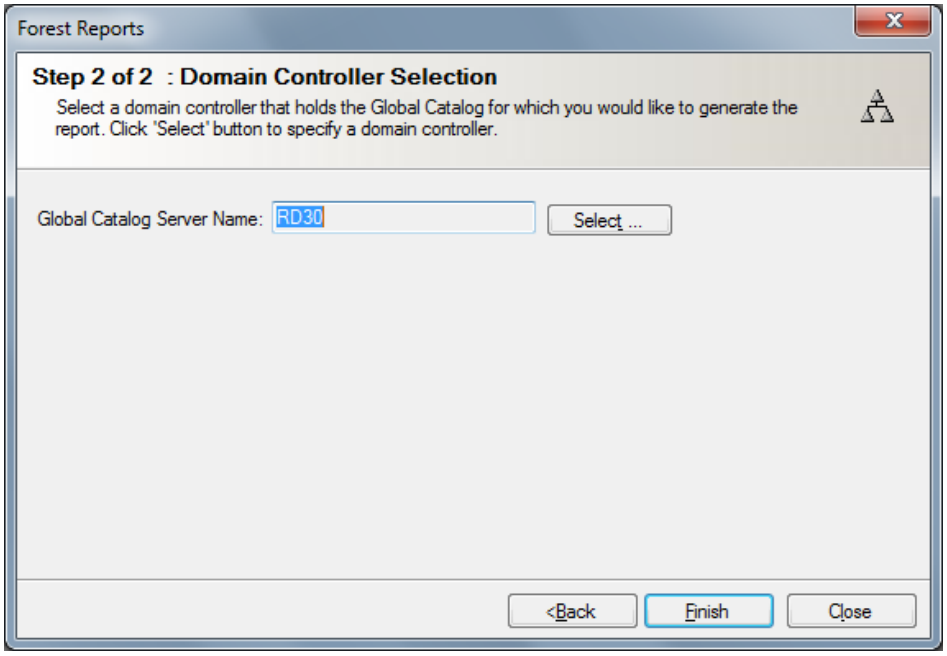
2) The **Forest Reports** window with the **list of reports** will be displayed as shown below:



3) This window shows the *list of reports* that can be generated across domains in a forest. Select a report from the list of reports.

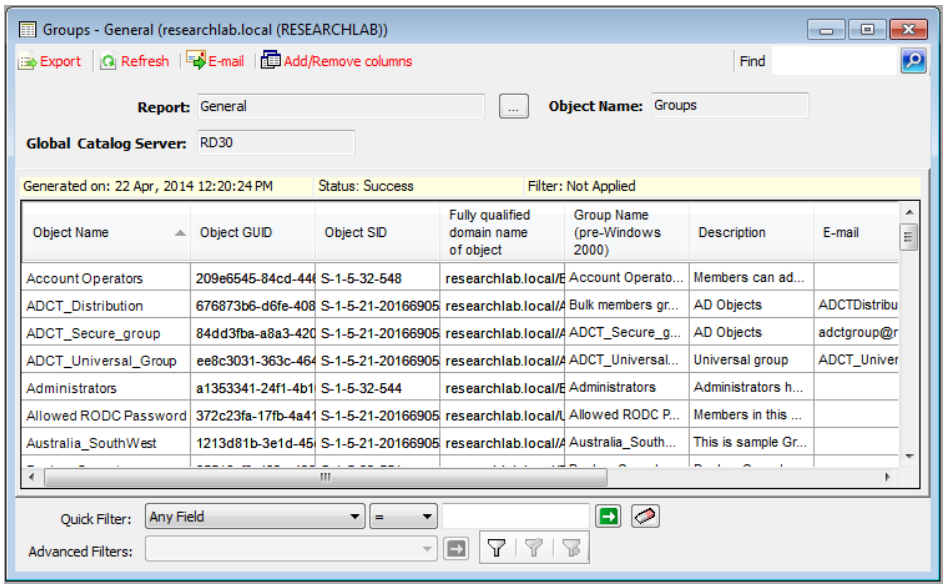
Click ***Next*** to proceed to the next step.

4) Specify a *domain controller* that holds the *Global Catalog* for which you want to generate the selected report. Please note that the domain controller that you specify must be a ***Global Catalog server*** for generating forest reports. Click ***Select*** button to specify a ***domain controller***. The Connection Manager will be displayed which will allow you to specify a domain controller.


Forest Reports
Step 2 of 2 : Domain Controller Selection
Select a domain controller that holds the Global Catalog for which you would like to generate the report. Click 'Select' button to specify a domain controller.
Global Catalog Server Name:
RD30
Select ...
<Back
Finish
Close

5) Click ***Finish*** to generate the report.

6) After the data collection process is complete, the report would be generated in a report window as shown below:



7) To generate another report across domains click on the ***browse*** button ("...") next to ***Report name*** in the report window.

Chapter 7

7 Permissions Reports

7.1 About Permissions Reports

The ***Permissions Reports*** feature in ARKAD allows the user to create user-defined reports for viewing permissions assigned to specific accounts on objects in the directory. Permissions Reports are categorized based on the type of permissions that they report, namely, Security Permissions and Auditing Permissions. Permissions Reports can be created for all objects that ARKAD reports on except for RSoP and Starter GPOs. In addition, these reports can be generated against specific containers for specific Users/Groups in a domain and additional criteria may be applied to get a narrow subset of data.

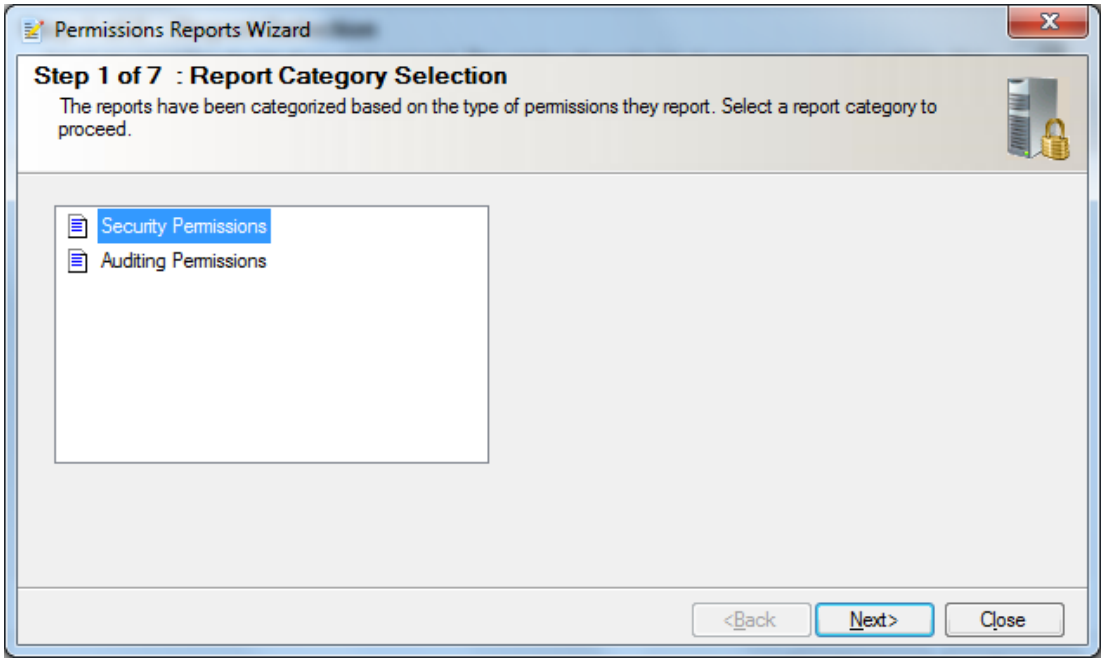
7.2 How to create Permissions Reports?

The ***Permissions Reports*** Wizard allows you to *create* or *edit* a permissions report. You can access the Permissions Reports Wizard from the Permissions Reports Window.

The Permissions Reports wizard will guide you through the following steps to create or edit a permissions report. During edit operation, however, the permissions report name and its report category cannot be modified.

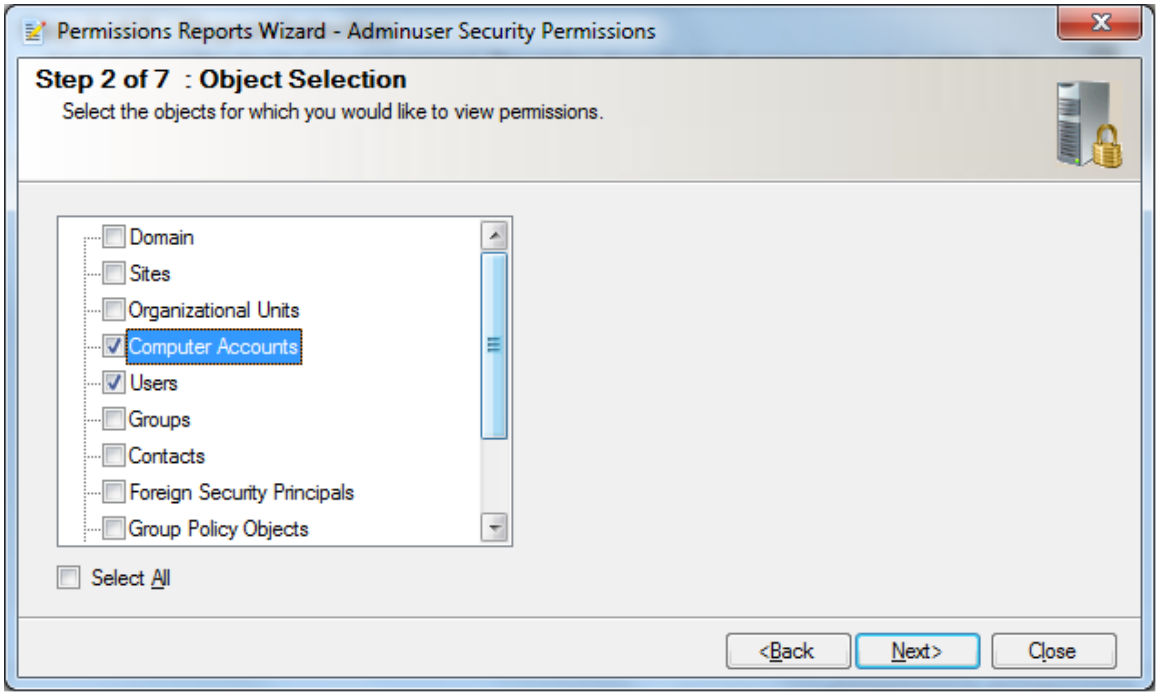
CHAPTER-7–Permissions Reports

Step 1: Report Category Selection


Permissions Reports Wizard
Step 1 of 7 : Report Category Selection
The reports have been categorized based on the type of permissions they report. Select a report category to proceed.
Security Permissions
Auditing Permissions
<Back
Next>
Close

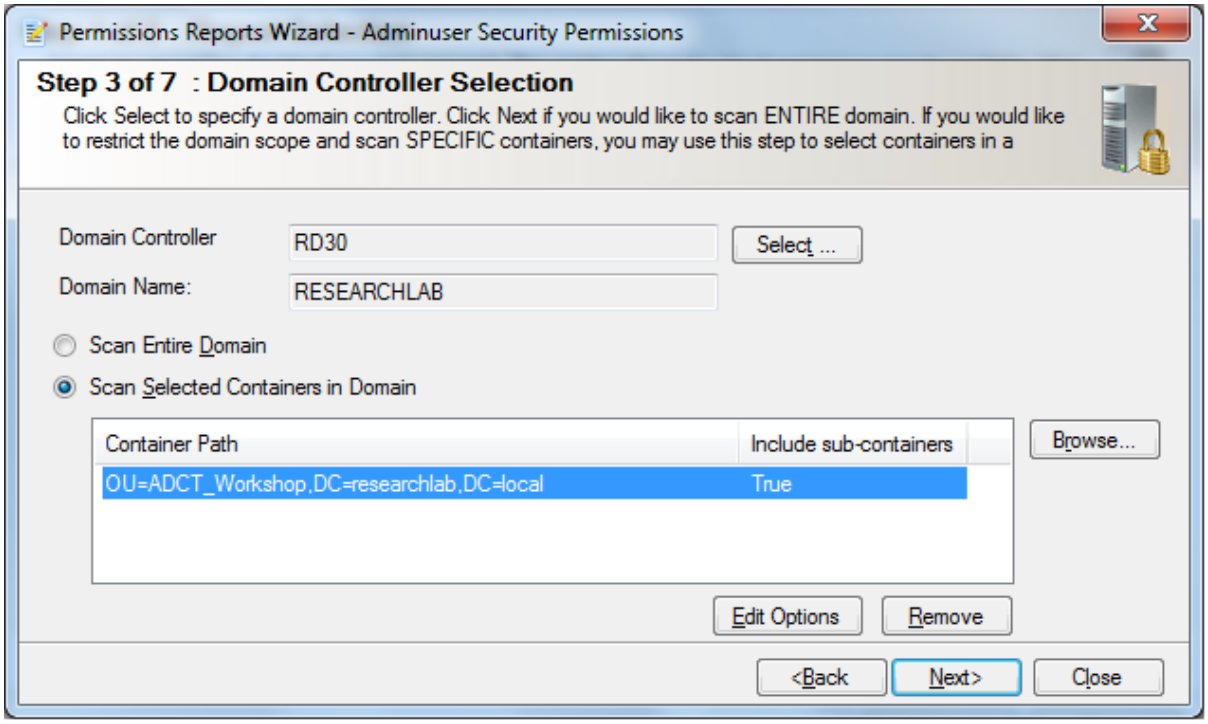
1) Select a ***report category*** from the list. You can select only one category. *Permissions Reports* are categorized based on the type of permissions they report. That is, ***Security Permissions*** category reports Security tab data, whereas, ***Auditing Permissions*** category reports Auditing tab data.
2) Click ***Next*** to proceed to the next step. You may Click *Back* button anytime to come back to a previous step.

Step 2: Object Selection

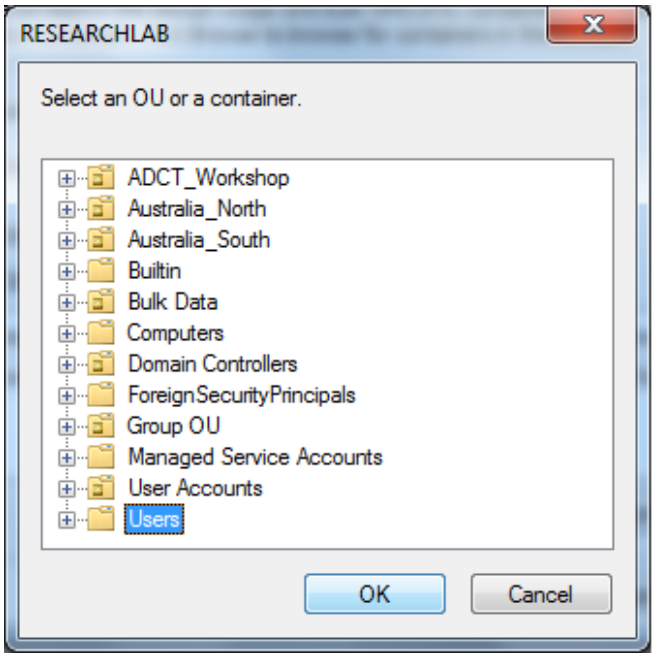


1) Select the desired ***object****(s)* from the list, using the *checkboxes*, for which you want to *view permissions* defined.
2) Click ***Next*** to proceed to the next step.

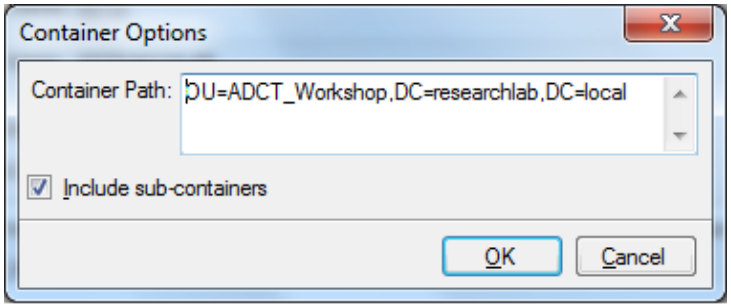
Step 3: Domain Controller Selection


Permissions Reports Wizard - Adminuser Security Permissions
Step 3 of 7 : Domain Controller Selection
Click Select to specify a domain controller. Click Next if you would like to scan ENTIRE domain. If you would like to restrict the domain scope and scan SPECIFIC containers, you may use this step to select containers in a
Domain Controller
RD30
Select ...
Domain Name:
RESEARCHLAB
Scan Entire Domain
Scan Selected Containers in Domain
Container Path
Include sub-containers
OU=ADCT_Workshop,DC=researchlab,DC=local
True
Browse...
Edit Options
Remove
<Back
Next>
Close

1) Click ***Select*** to specify a **domain controller** and corresponding domain for which you want the report generated. The *Connection Manager* will be displayed which will allow you to specify a *domain controller*. Note that the report can be generated only against the domain you specify in this step. During report generation you may specify any domain controller that belongs to the selected domain.
2) You may select *specific containers* in the domain to restrict the domain scope and collect data for objects in selected containers. If no containers are selected, data will be collected by searching the entire domain structure.
3) In order to select specific containers, select ***Scan Selected Containers in Domain*** option, and then click ***Browse*** to select containers in the domain.
4) The container browser dialog will be displayed as shown below:

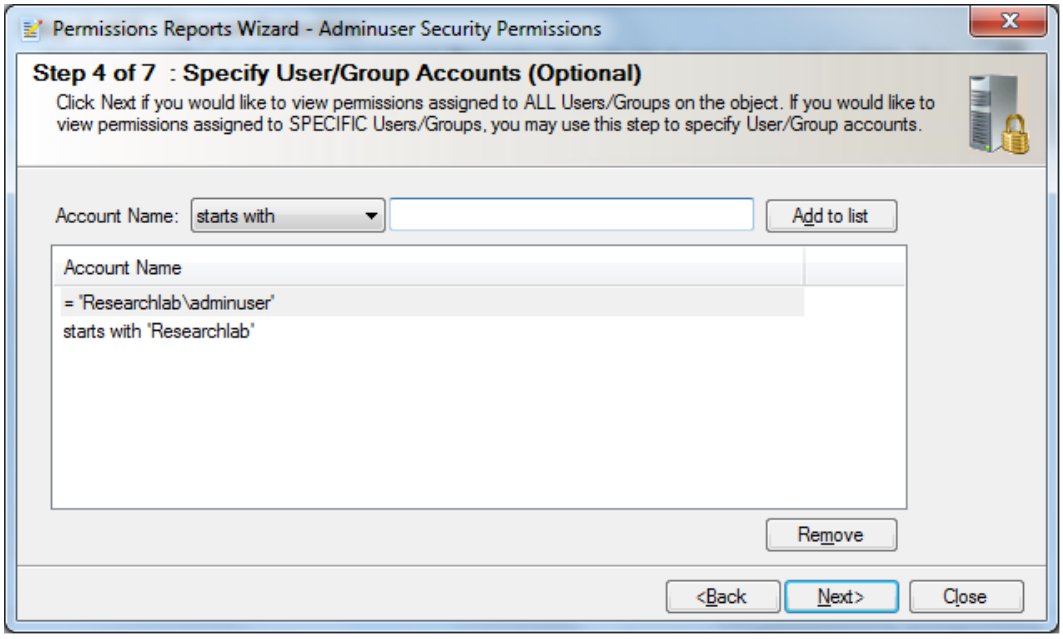


5) *Select* the desired *container* and click ***OK.*** Note that only one container may be selected at a time. To select another container, click ***Add From.*** Note that ARKAD scans the specified container for the objects selected in Step 2 of this wizard
6) ARKAD defaults to scanning all the sub-containers under a given container. If you want to change the Include sub-containers option click *Edit Options***.** The ***Container Options*** dialog will be displayed as shown below:



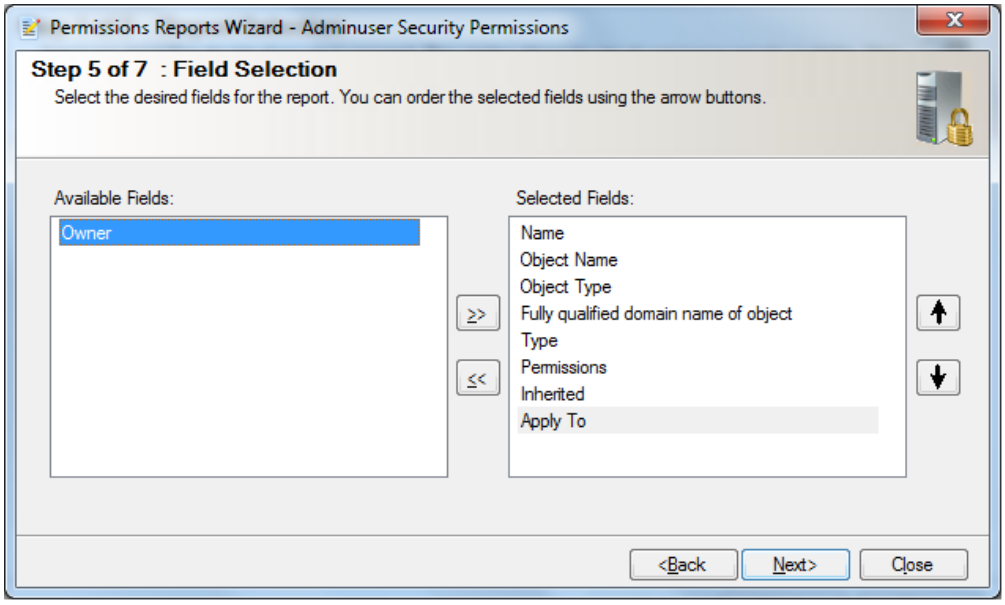
6) Please ***Note*** that Container Selection is not applicable for Domain, Sites, GPOs and WMI Filters.
7) Click ***Next*** to proceed to the next step.

Step 4: Specify User/Group Accounts (Optional)


Permissions Reports Wizard - Adminuser Security Permissions
Step 4 of 7 : Specify User/Group Accounts (Optional)
Click Next if you would like to view permissions assigned to ALL Users/Groups on the object. If you would like to view permissions assigned to SPECIFIC Users/Groups, you may use this step to specify User/Group accounts.
Account Name:
starts with
Add to list
Account Name
= 'Researchlab\adminuser'
starts with 'Researchlab'
Remove
<Back
Next>
Close

1) ***Specify user*** and/or ***group account names*** to view permissions assigned to specific accounts on objects in the directory.
2) Select an *operator* from the drop-down list, and then specify an account name to add to the list. You may specify a part of ***account name*** to include in list by using operators other than equals (=) and not equals (<>). Note that for equals and not equals operators you have to specify account name in "Domain Name\Account Name" format.
3) Click ***Add to list*** to add the specified account name to list.
4) Click ***Next*** to proceed to the next step.

Step 5: Field Selection



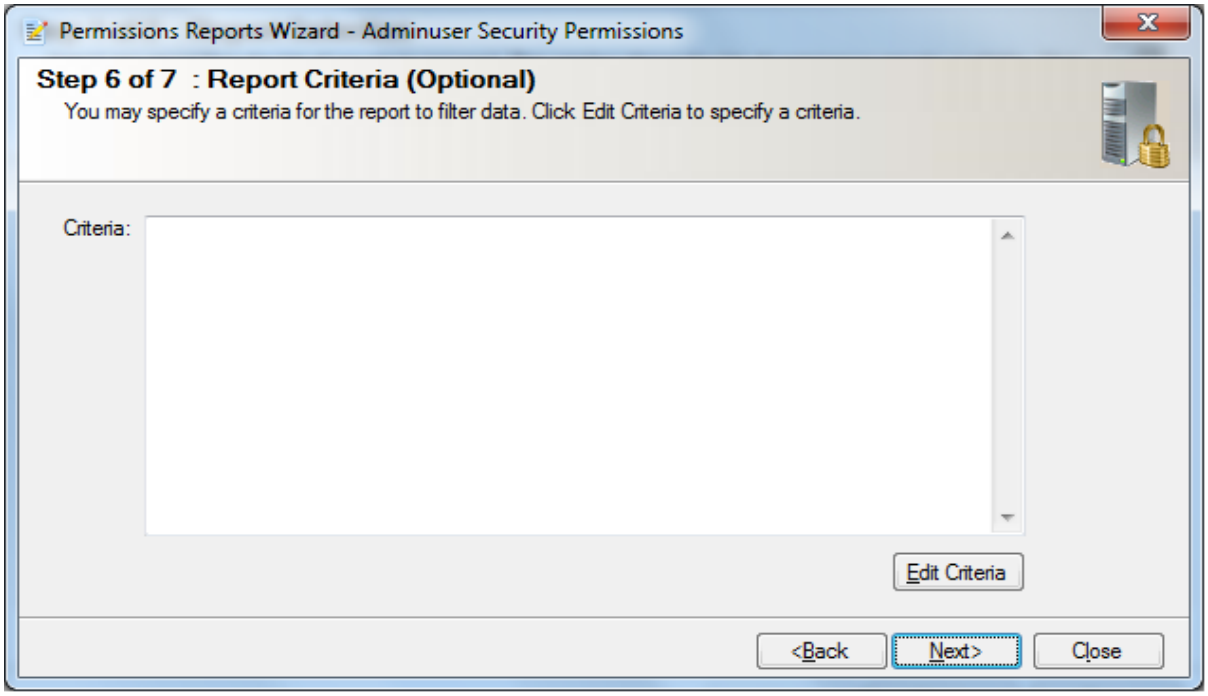
1) To select fields for the report, click on the *desired field* in the list of ***Available Fields***, and then *click* >> *button.*

2) To *remove selected fields*, click on the desired field in the list of ***Selected Fields,*** and then *click* << *button.*

3) You can use the ***arrow buttons*** to order the selected fields. To move a ***field up*** by one position in the list of selected fields *click* ↑ *button.* To move a ***field down*** by one position in the list of selected fields *click* ↓ *button.*

4) Click ***Next*** to proceed to the next Step.

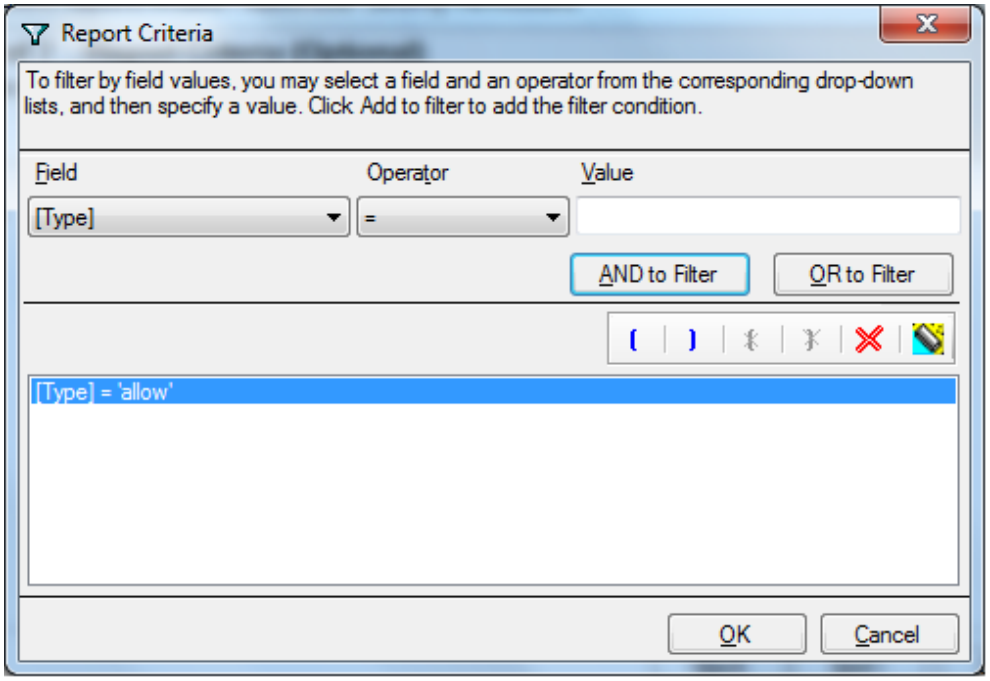
Step 6: Report Criteria (Optional)


Permissions Reports Wizard - Adminuser Security Permissions
Step 6 of 7 : Report Criteria (Optional)
You may specify a criteria for the report to filter data. Click Edit Criteria to specify a criteria.
Criteria:
Edit Criteria
<Back
Next>
Close

This step allows you to apply **report criteria** by specifying conditions for filtering report data.

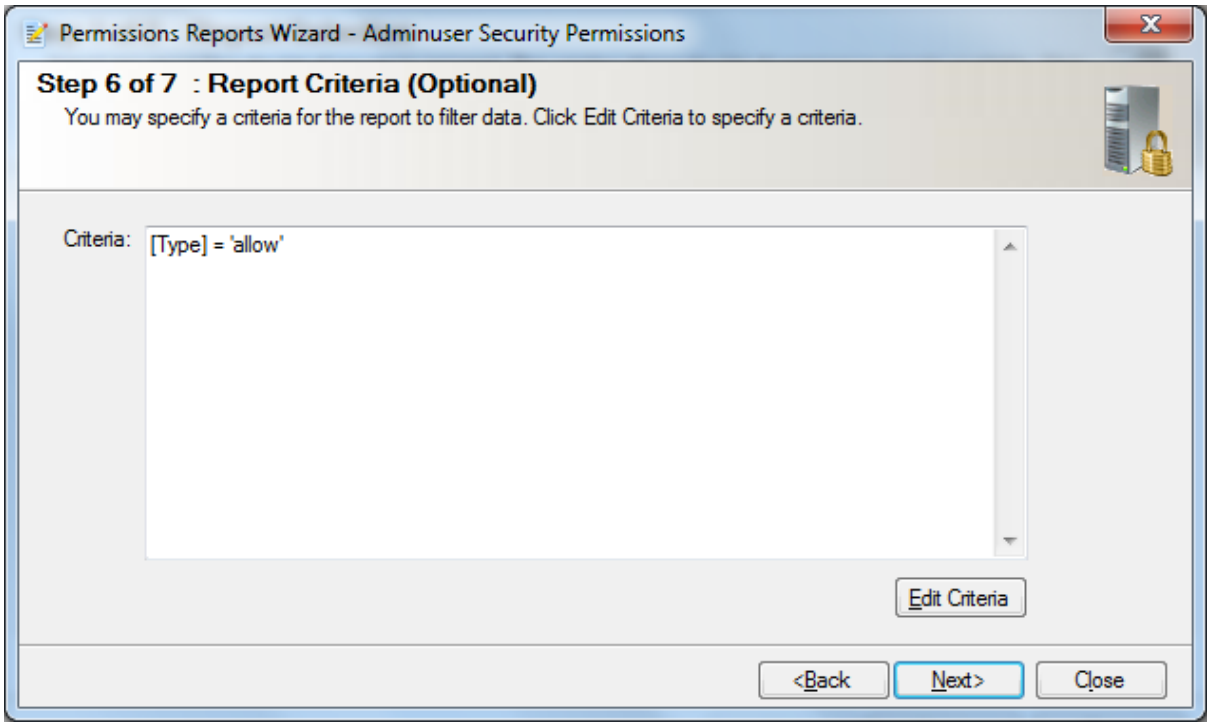
1) To set a *criteria* for the report, click ***Edit Criteria*****.**
2) The ***Report Criteria*** window shows up on screen. *Select* a ***field***, an ***operator,*** and specify a ***value*** for the condition. **Click** Add to filter button to add the filter condition.

The ***Report Criteria*** window is shown below:


Report Criteria
To filter by field values, you may select a field and an operator from the corresponding drop-down lists, and then specify a value. Click Add to filter to add the filter condition.
Field
Operator
Value
[Type]
=
AND to Filter
OR to Filter
[Type] = 'allow'
OK
Cancel

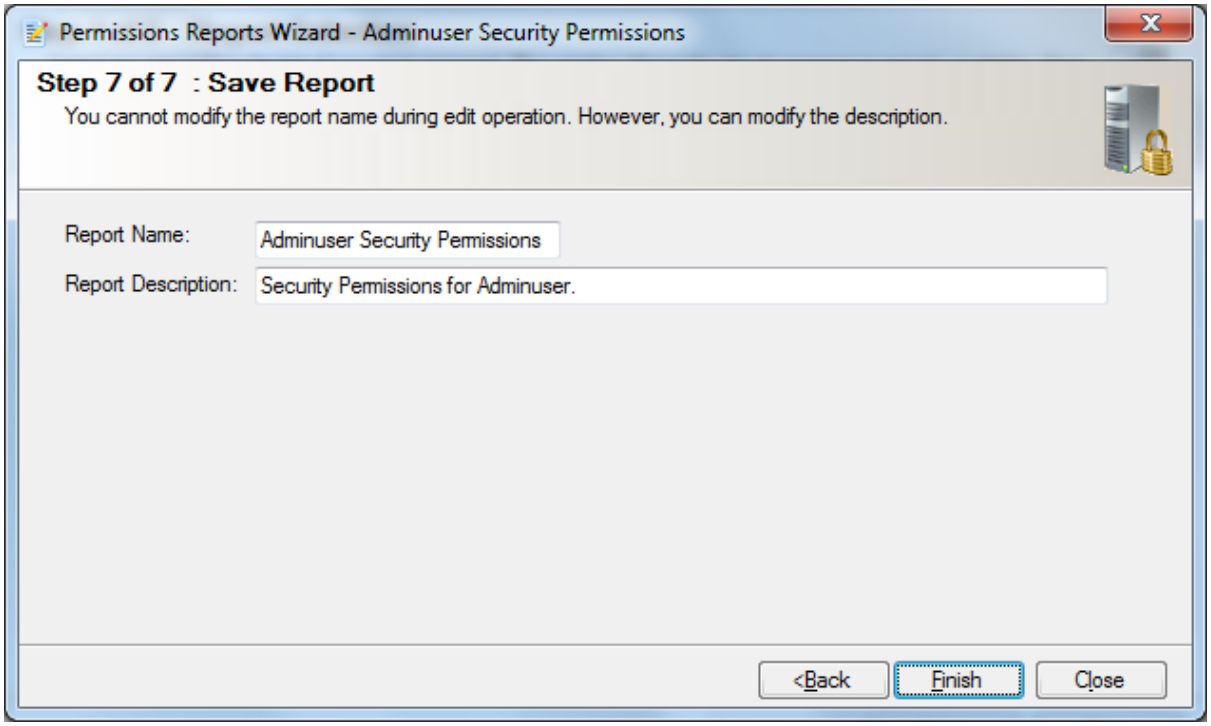
3) Click ***OK*** *t*o apply the criteria to the report.

4) The applied ***Report criteria*** would be displayed as shown below:


Permissions Reports Wizard - Adminuser Security Permissions
Step 6 of 7 : Report Criteria (Optional)
You may specify a criteria for the report to filter data. Click Edit Criteria to specify a criteria.
Criteria:
[Type] = 'allow'
Edit Criteria
<Back
Next>
Close

5) Click ***Next*** to proceed to the next Step.

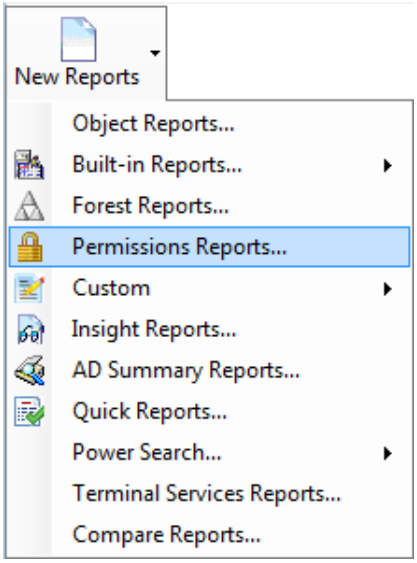
Step 7: Save Report


Permissions Reports Wizard - Adminuser Security Permissions
Step 7 of 7 : Save Report
You cannot modify the report name during edit operation. However, you can modify the description.
Report Name:
Adminuser Security Permissions
Report Description:
Security Permissions for Adminuser.
<Back
Finish
Close

1) **Enter a name** and description for the **permissions report.**
2) Click ***Finish*** to save the permissions report.

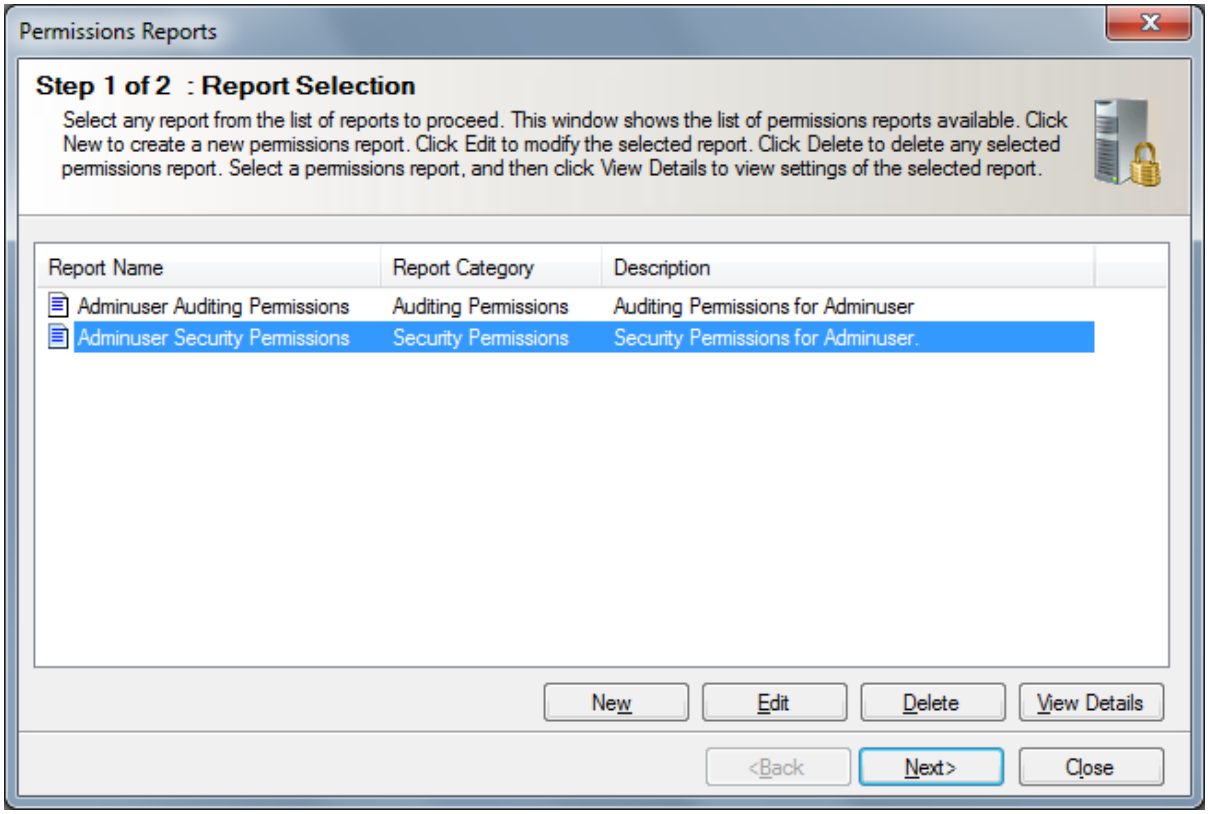
7.3 How to generate Permissions Reports?

Perform the following steps to generate a ***permissions report.***

1) ***Select*** 

under *New Report* button in the tool bar.

2) The ***Permissions Reports*** window with the list of available permissions reports will be displayed as shown below:


Permissions Reports
Step 1 of 2 : Report Selection
Select any report from the list of reports to proceed. This window shows the list of permissions reports available. Click New to create a new permissions report. Click Edit to modify the selected report. Click Delete to delete any selected permissions report. Select a permissions report, and then click View Details to view settings of the selected report.
Report Name
Report Category
Description
Adminuser Auditing Permissions
Auditing Permissions
Auditing Permissions for Adminuser
Adminuser Security Permissions
Security Permissions
Security Permissions for Adminuser.
New
Edit
Delete
View Details
<Back
Next>
Close

3) *Select a report* from the list of reports.

You can create a ***new*** **permissions report** by clicking **New** button. This will launch the ***Permissions Reports*** Wizard which will guide you through the steps for creating a permissions report.

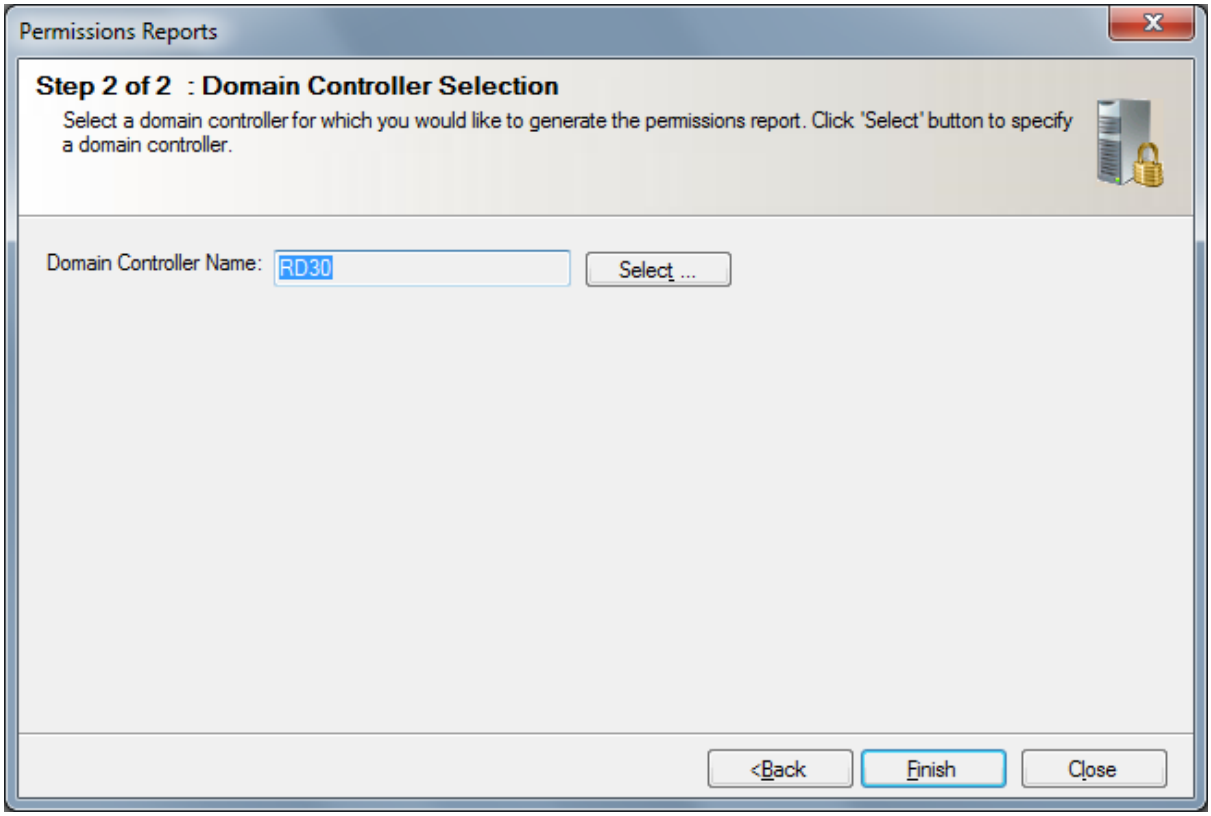
To ***modify*** an existing permissions report, select a report, and then click ***Edit*** button. The ***Permissions Reports*** *Wizard* will be displayed which will guide you through the steps for *editing a permissions report.*

Click ***Delete*** button to *delete* any selected *permissions report*. Please note that you cannot delete a permissions report which currently is being viewed.

You can *view the settings* for any selected report by clicking ***View Details*** button.

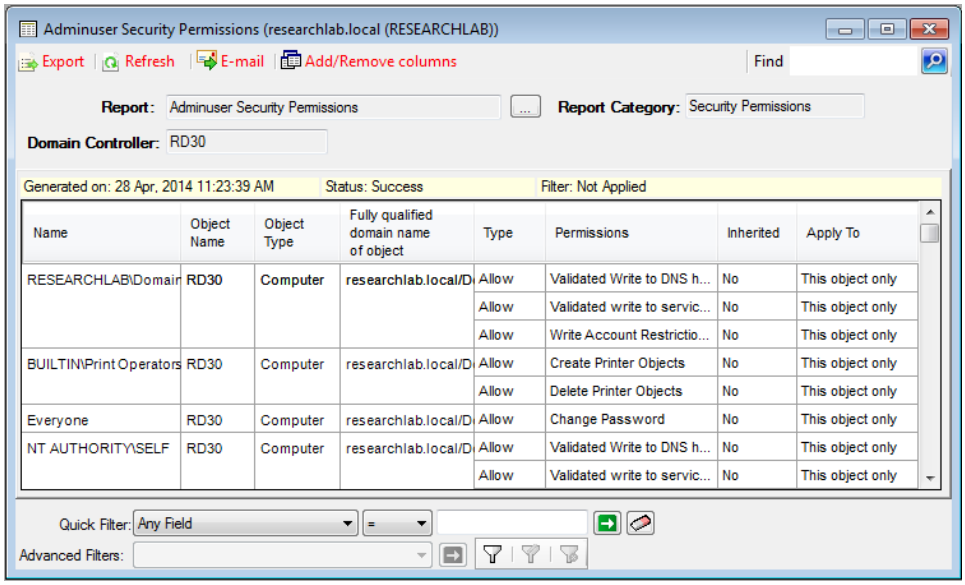
Click ***Next*** to proceed to the next step.

4) By default, ARKAD uses the *domain controller* specified during Permissions Report creation process for report generation. However, you may specify a different domain controller against which you want the selected permissions report generated. Note that the domain controller you specify must belong to the same domain to which the selected permissions report is associated. Click **Select** button to ***specify a domain controller.*** The Connection Manager will be displayed which will allow you to specify a domain controller.


Permissions Reports
Step 2 of 2 : Domain Controller Selection
Select a domain controller for which you would like to generate the permissions report. Click 'Select' button to specify a domain controller.
Domain Controller Name:
RD30
Select ...
<Back
Finish
Close

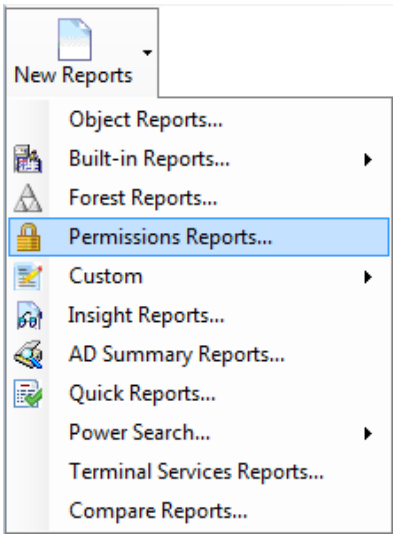
5) Click ***Finish*** to generate the report.

6) After the data collection process is complete, the report would be generated in a report window as shown below:

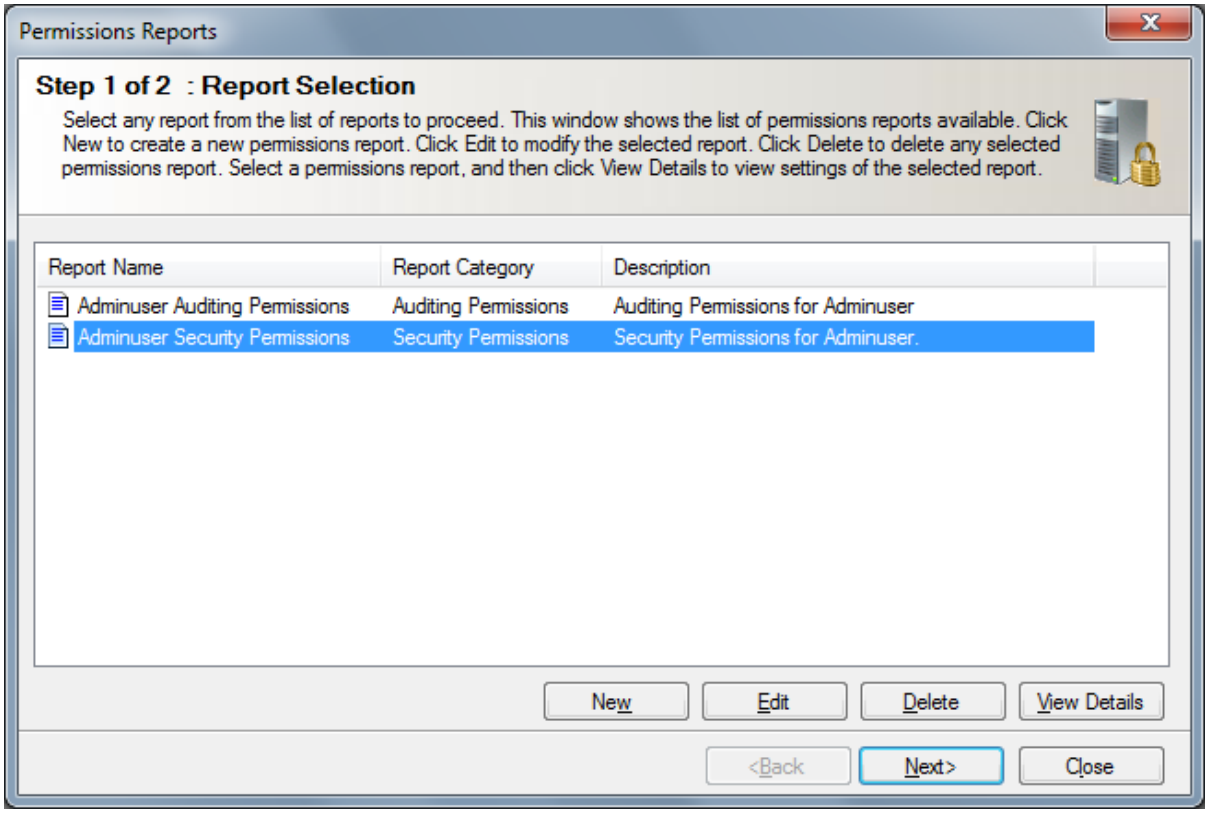


7) To generate another permissions report, click on *the* ***browse*** button ("...") next to Report name in the report window.

7.4 How to Manage Permissions Reports?



Click under *New Report* button in the tool bar to launch the ***Permissions Reports*** Window. The *Permissions Reports* Window shows the list of permissions reports available. The ***Report Category*** column shows the type of permissions reported.


Permissions Reports
Step 1 of 2 : Report Selection
Select any report from the list of reports to proceed. This window shows the list of permissions reports available. Click New to create a new permissions report. Click Edit to modify the selected report. Click Delete to delete any selected permissions report. Select a permissions report, and then click View Details to view settings of the selected report.
Report Name
Report Category
Description
Adminuser Auditing Permissions
Auditing Permissions
Auditing Permissions for Adminuser
Adminuser Security Permissions
Security Permissions
Security Permissions for Adminuser.
New
Edit
Delete
View Details
<Back
Next>
Close

The *Permissions Reports* Window allows you to perform the following operations:

- ***Create*** a new Permissions Report
- ***Edit*** an existing Permissions Report
- ***Delete*** a Permissions Report
- ***View settings*** for a Permissions Report

CHAPTER-7–Permissions Reports

- ***Generate*** a Permissions Report

Create a new Permissions Report

1) To *create* a *new* permissions report click ***New*** button in the ***Permissions Reports*** Window. The Permissions reports Wizard will appear on the screen.
2) Follow the steps as outlined in How to create Permissions reports?

Edit an existing Permissions report

1) To ***edit*** permissions report click ***Edit*** button in the ***Permissions Reports*** Window. The Permissions reports Wizard will appear on the screen which will guide you through the edit operation.
2) During the edit operation you can modify the list of objects, User/Group accounts, AD containers, fields that make up the permissions report and the report's description.

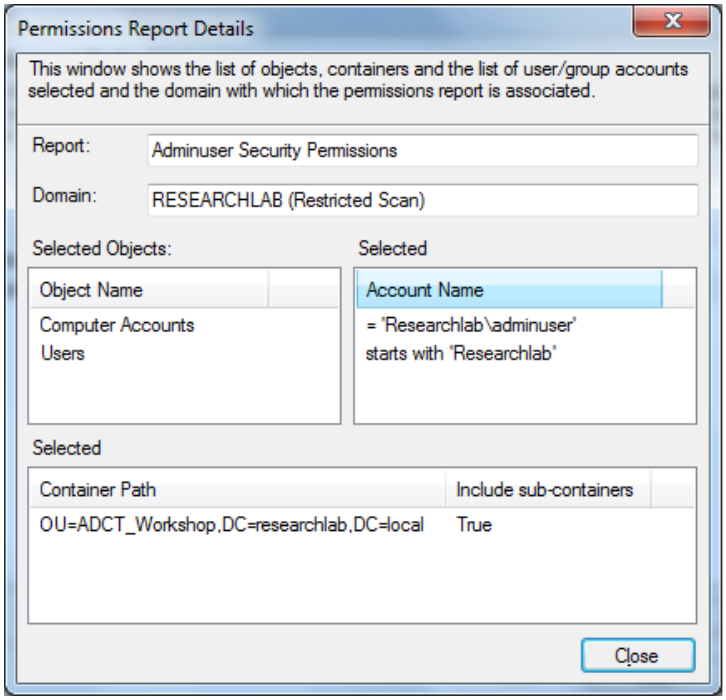
Delete a permissions report

To *delete* a *permissions report*, ***select*** the report you want to ***delete,*** and then click ***Delete*** button. The selected permissions report and all its associated saved filters, if any, will be deleted ***permanently.*** Further, the permissions report will be removed from scheduled tasks, if any, already scheduled.

View settings for a permissions report

To *view details* of a permissions report ***select*** the report, and then click ***View Details*** button. The selected ***permissions report's details*** would be shown as below:

CHAPTER-7–Permissions Reports



The ***Details*** window shows the ***report name, the domain name*** with which the report is associated, the ***list of objects, User/Group accounts***, and the ***list of AD containers*** selected.

Generate a permissions report

To generate a permissions report follow the steps as outlined in How to generate Permissions reports?

Chapter 9

8 Custom Reports

8.1 About Custom Reports

The ***Custom Reports*** feature in ARKAD allows the user to *create* own *custom made reports* (user-defined) from one or more Object Reports (each tab view in the report view window of an object is termed an Object Report).

Custom reports can be created by including fields of the same object (fields from one or more Object Reports within any single object) that ARKAD reports on. The source object from which the lists of fields are defined for the custom report is the "Object Category" of the custom report.

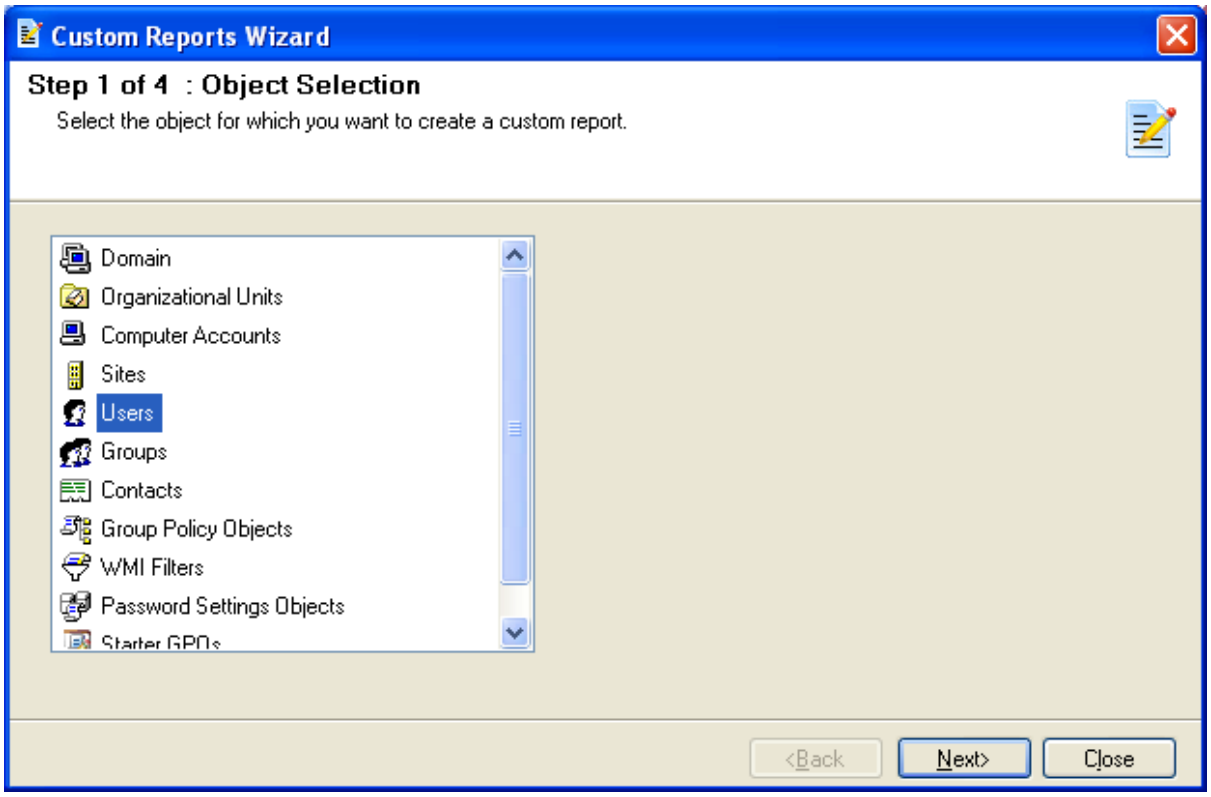
Currently, custom reports can be created for all objects that ARKAD reports on except for RSoP. In addition, a custom report can be created by combining all Object Reports except for "Deleted Objects" report.

8.2 How to create Custom Reports?

The ***Custom Reports*** Wizard allows you to ***create or edit*** a custom report. You can access the *Custom Reports Wizard* from the Connection Manager.

The *Custom Reports wizard* will guide you through the following steps to create or edit a custom report. During edit operation, however, the custom report name and its object category cannot be modified.

Step 1: Object Selection

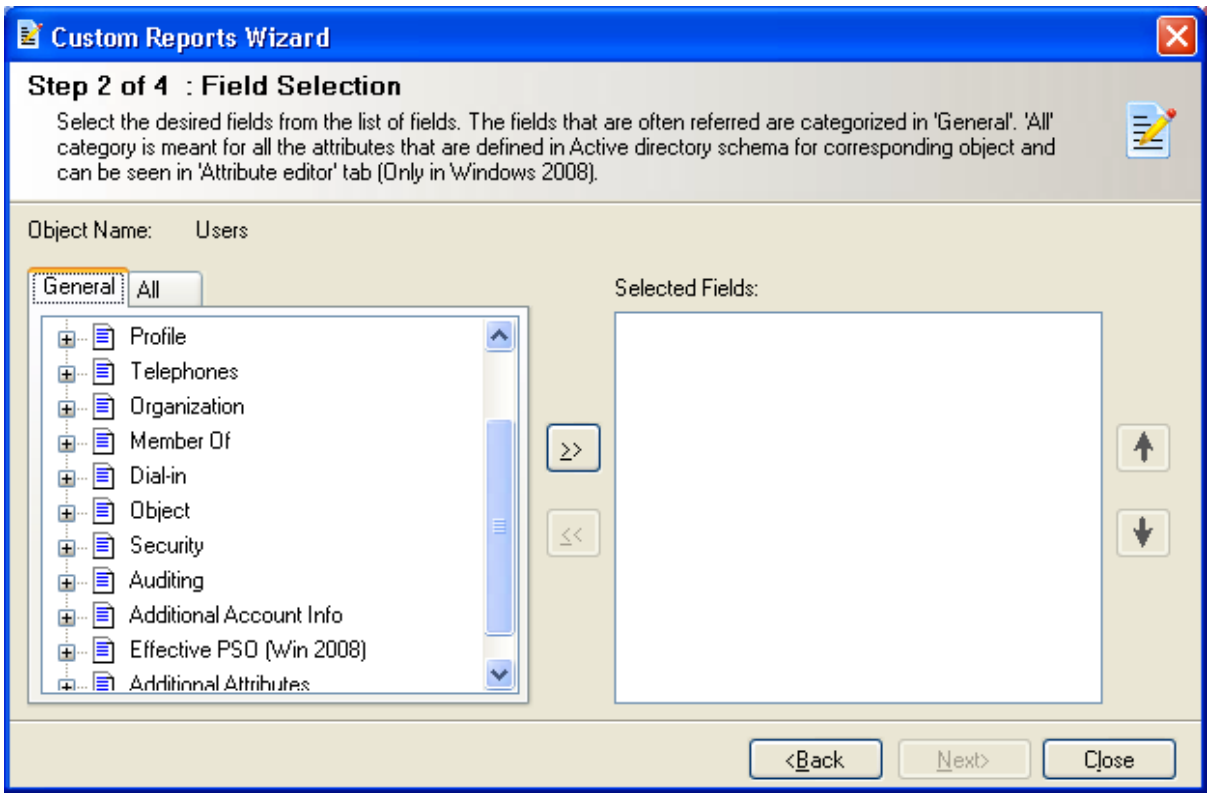


1) ***Select*** *an* ***object*** from the list of objects. You can select only one object from the list. The selected object will be the "Object Category" of the custom report. Also, you will be able to select fields only from reports pertaining to the object selected in this step. However, you can always come back to this step and select another object. Note that doing so will remove all fields selected earlier.
2) Click ***Next*** to proceed to the next step. You may Click *Back* button anytime to come back to a previous step.

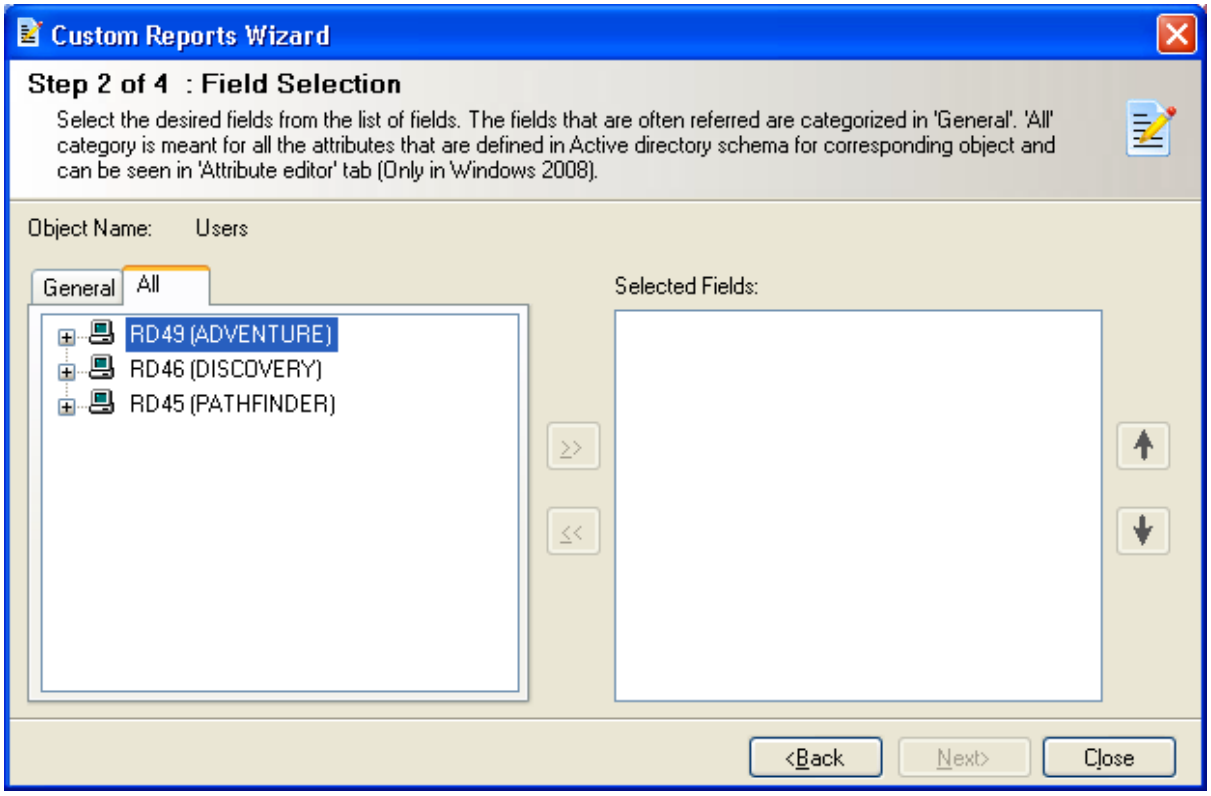
Step 2: Field Selection

Overview:

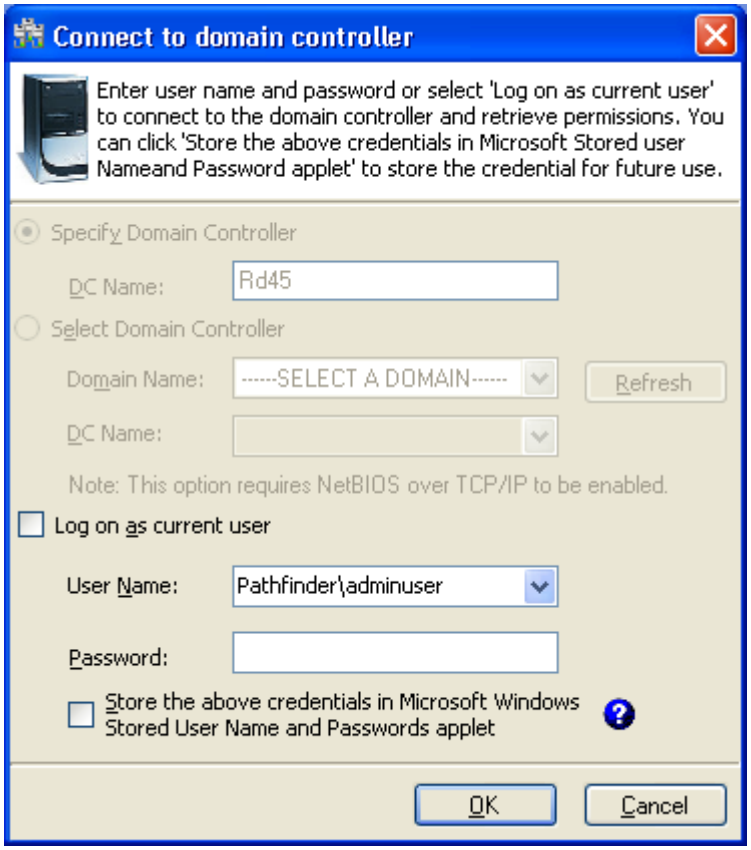
The fields (attributes) pertaining to the selected object will be displayed under General and All categories. The list of fields shown as tabs in Active Directory console and schema will be displayed under 'General' and 'All' tabs respectively.


Custom Reports Wizard
Step 2 of 4 : Field Selection
Select the desired fields from the list of fields. The fields that are often referred are categorized in 'General'. 'All' category is meant for all the attributes that are defined in Active directory schema for corresponding object and can be seen in 'Attribute editor' tab (Only in Windows 2008).
Object Name: Users
General
All
Profile
Telephones
Organization
Member Of
Dial-in
Object
Security
Auditing
Additional Account Info
Effective PSO (Win 2008)
Selected Fields:
>>
<<
<Back
Next>
Close

When 'All' tab is selected, the list of domain controllers in the Connection Manager is populated as shown below. You can select any attribute in AD schema of the desired domain controller. If a domain controller is not connected in Connection Manager, then the corresponding domain controller needs to be authenticated in the Connect to domain controller dialog.


Custom Reports Wizard
Step 2 of 4 : Field Selection
Select the desired fields from the list of fields. The fields that are often referred are categorized in 'General'. 'All' category is meant for all the attributes that are defined in Active directory schema for corresponding object and can be seen in 'Attribute editor' tab (Only in Windows 2008).
Object Name: Users
General
All
RD49 (ADVENTURE)
RD46 (DISCOVERY)
RD45 (PATHFINDER)
Selected Fields:
<Back
Next>
Close

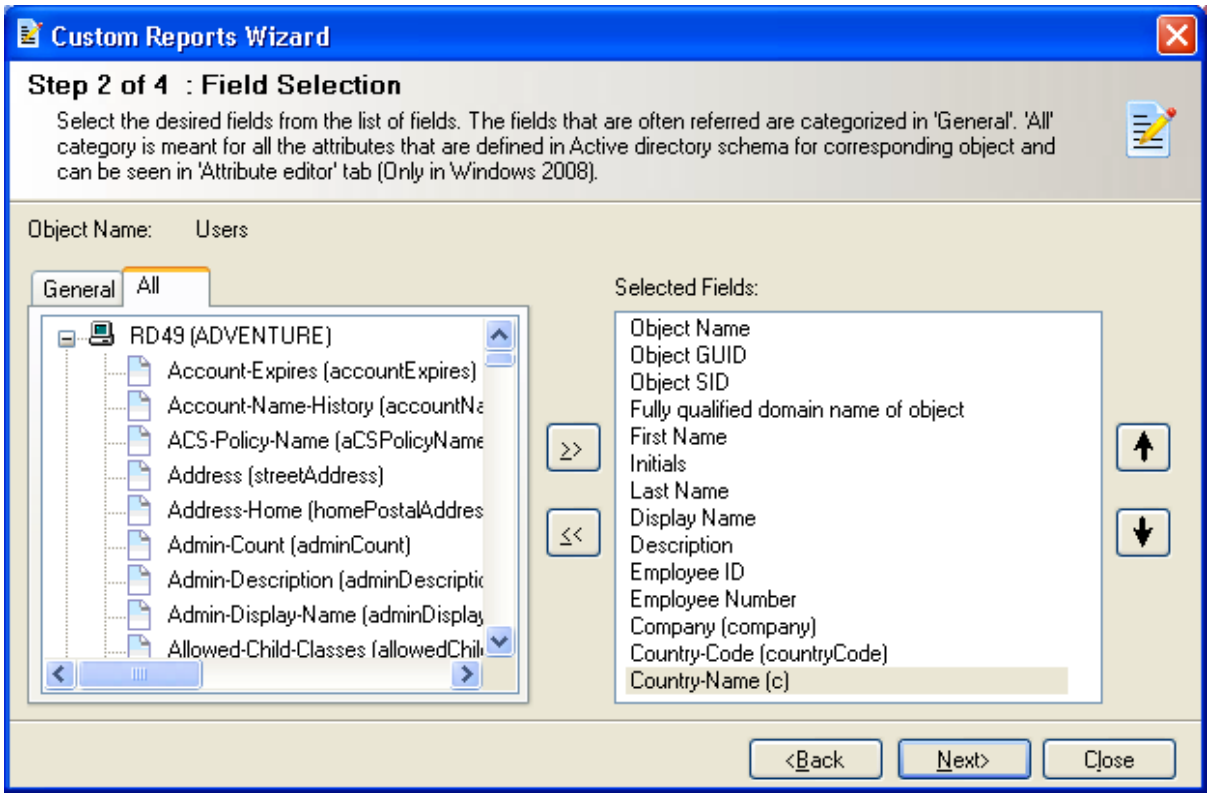
Connect to domain controller


Connect to domain controller
Enter user name and password or select 'Log on as current user' to connect to the domain controller and retrieve permissions. You can click 'Store the above credentials in Microsoft Stored user Nameand Password applet' to store the credential for future use.
Specify Domain Controller
DC Name:
Rd45
Select Domain Controller
Domain Name:
-----SELECT A DOMAIN-----
Refresh
DC Name:
Note: This option requires NetBIOS over TCP/IP to be enabled.
Log on as current user
User Name:
Pathfinder\adminuser
Password:
Store the above credentials in Microsoft Windows Stored User Name and Passwords applet
OK
Cancel

Right click on corresponding domain controller provides options such as 'Connect' or 'Refresh' to connect to the domain controller again and retrieve the attributes afresh.

Right click on the area other than domain controller node in 'All' category, presents 'Connection manager' and 'Refresh' options. These options can be used to launch Connection Manager and refresh the list of domain controllers respectively.

Steps:



1) To ***select fields*** from a report, click on the desired field in the list of ***Available Fields,*** and then *click* >> ***button.***

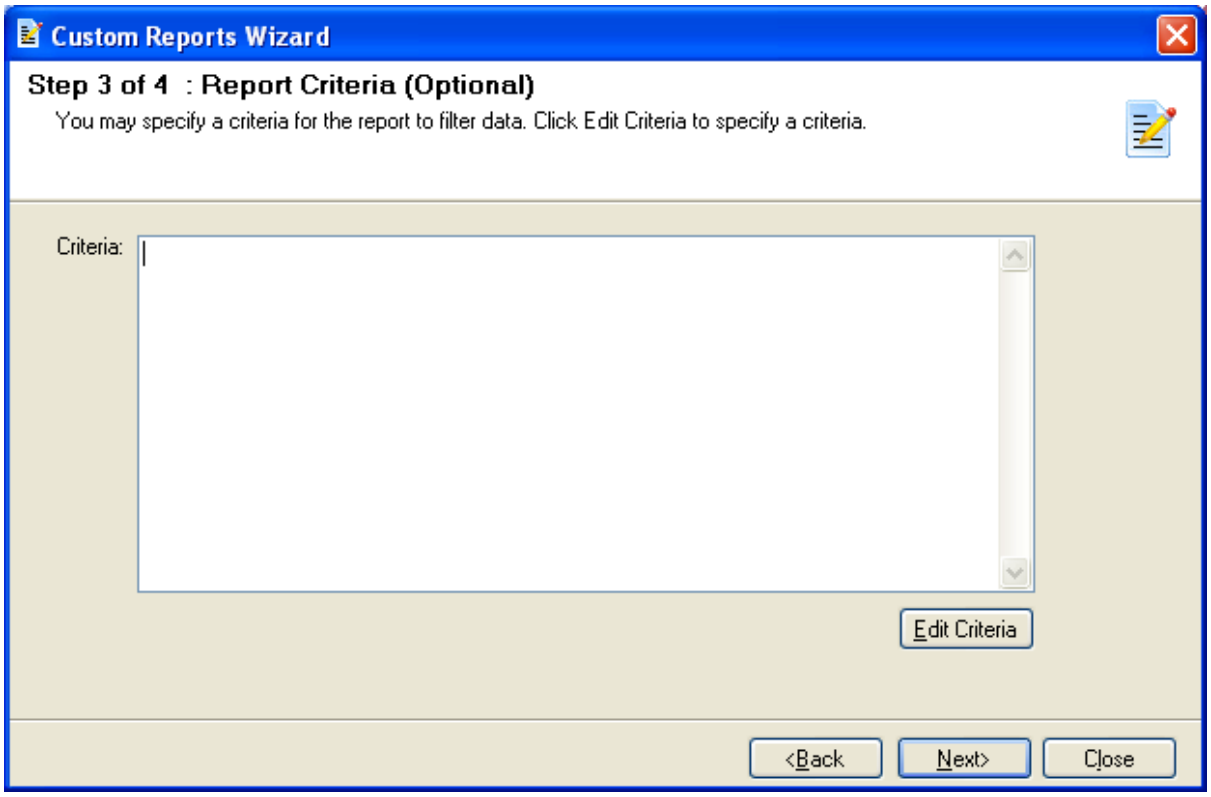
2) To ***remove selected fields***, click on the desired field in the list of Selected Fields, and then *click* << ***button.***

3) You can use the ***arrow*** buttons to **order** the selected fields. To move a ***field up*** by one position in the list of selected fields *click* ↑ ***button.*** To move a ***field down*** by one position in the list of selected fields *click* ↓ ***button.***

4) To choose fields from another report, select the desired report from the Report Name drop-down list, and then perform the above mentioned steps.

5) Click ***Next*** to proceed to the next Step.

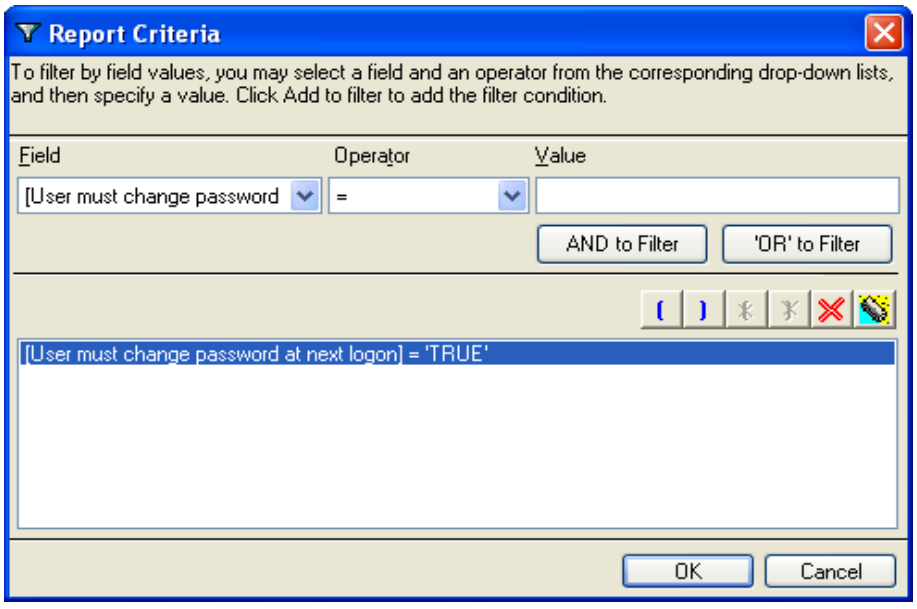
Step 3: Report Criteria (Optional)


Custom Reports Wizard
Step 3 of 4 : Report Criteria (Optional)
You may specify a criteria for the report to filter data. Click Edit Criteria to specify a criteria.
Criteria:
Edit Criteria
<Back
Next>
Close

This step allows you to ***apply report criteria*** by specifying conditions for *filtering report data.*

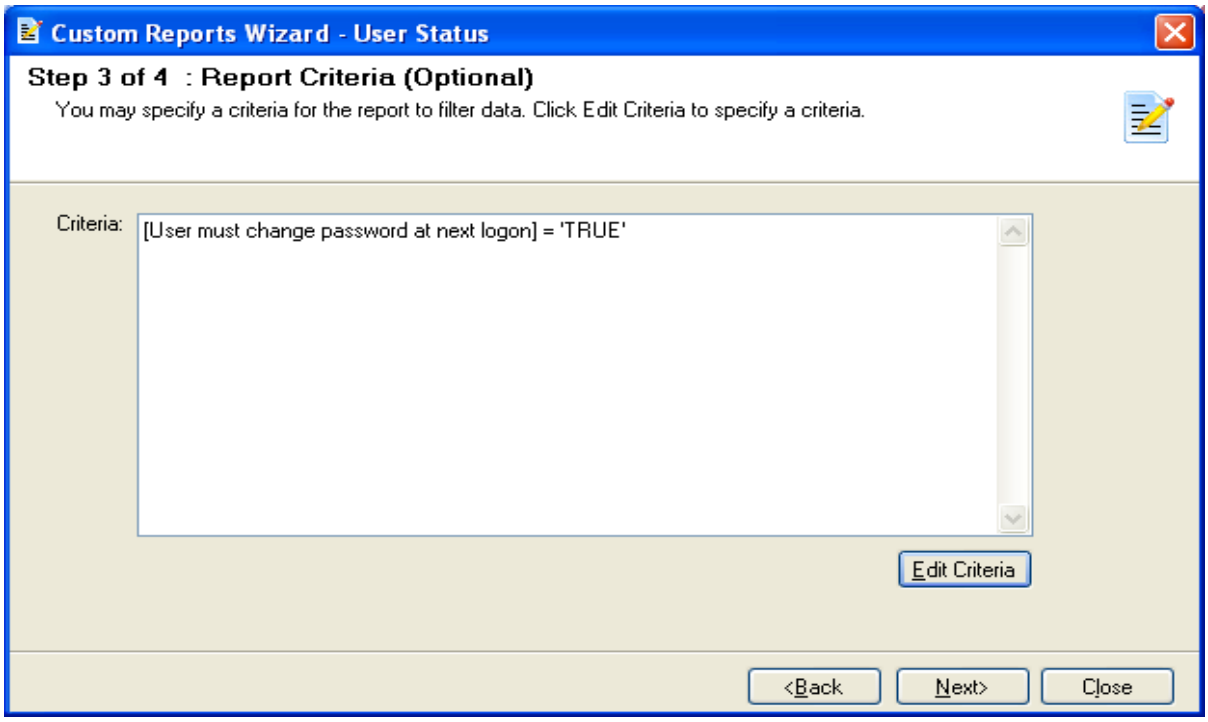
1) To *set* a criteria for the report, click ***Edit Criteria.***

2) The ***Report Criteria*** window shows up on screen. Select a ***field,*** an ***operator,*** and specify a ***value*** for the condition. Click Add to filter button to add the filter condition. The Report Criteria windows is shown below:


Report Criteria
To filter by field values, you may select a field and an operator from the corresponding drop-down lists, and then specify a value. Click Add to filter to add the filter condition.
Field
Operator
Value
[User must change password
=
AND to Filter
'OR' to Filter
[User must change password at next logon] = 'TRUE'
OK
Cancel

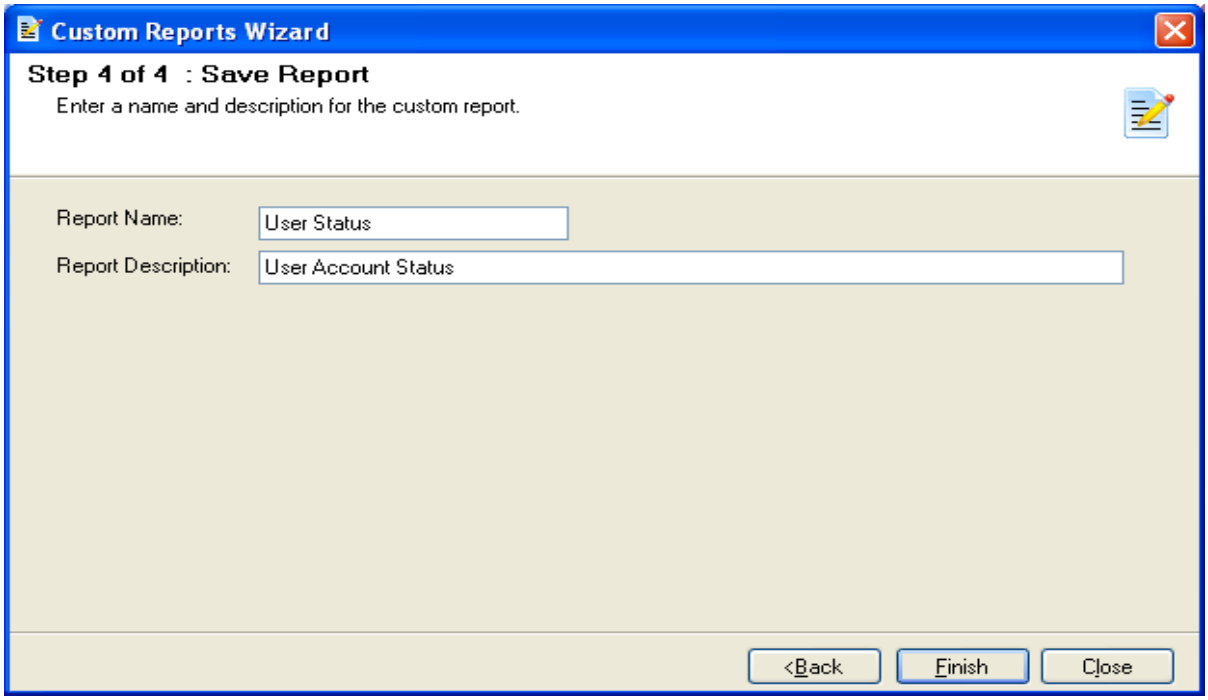
3) Click **OK** to apply the criteria to the report.

4) The applied ***report criteria*** would be displayed as shown below:


Custom Reports Wizard - User Status
Step 3 of 4 : Report Criteria (Optional)
You may specify a criteria for the report to filter data. Click Edit Criteria to specify a criteria.
Criteria:
[User must change password at next logon] = 'TRUE'
Edit Criteria
<Back
Next>
Close

5) Click ***Next*** to proceed to the next Step.

Step 4: Save Report

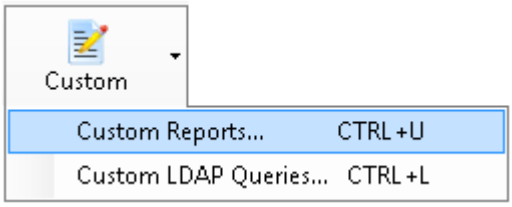


1) Enter a ***name*** and ***description*** for the ***custom report.***

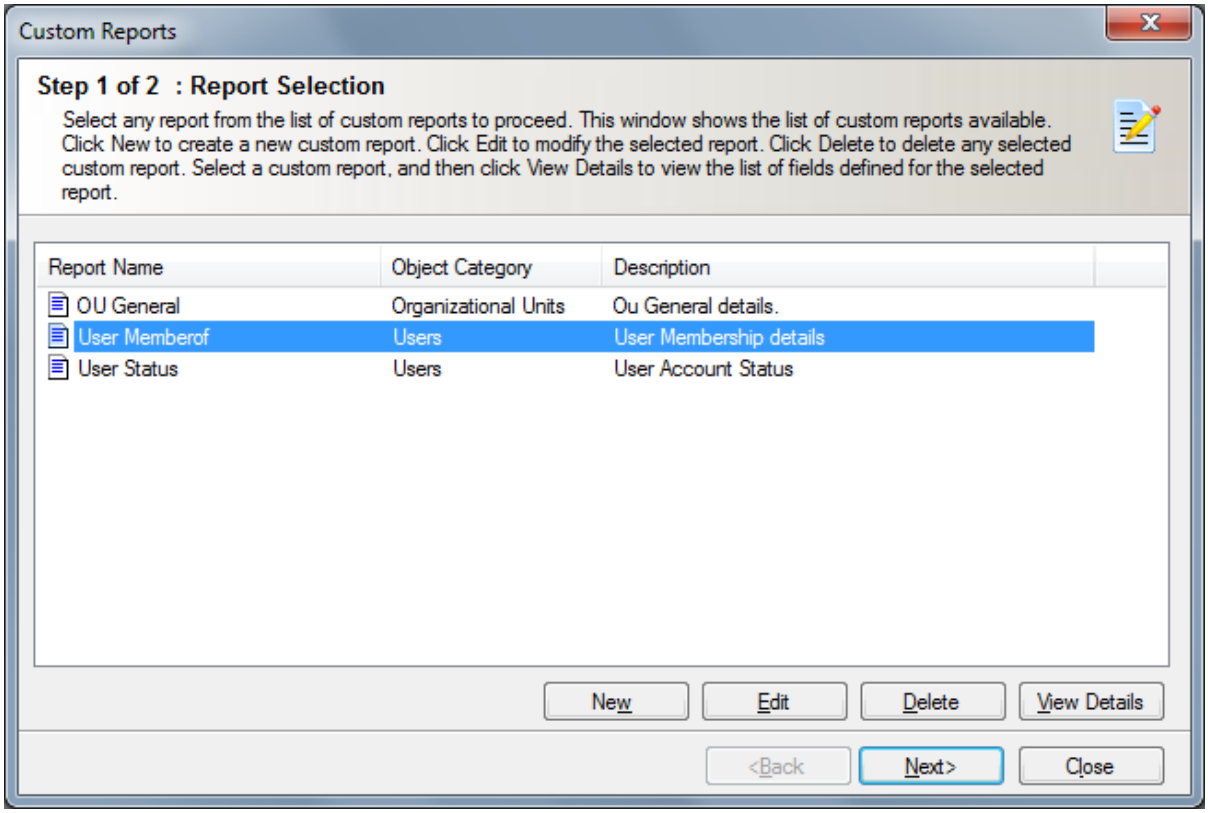
2) Click ***Finish*** to save the custom report.

8.3 How to generate Custom Reports?

Perform the following steps to ***generate*** *a* ***custom report.***

1) ***Select*** 

Menu in the toolbar.
2) The ***Custom Reports*** window with the list of available custom reports will be displayed as shown below:


Custom Reports
Step 1 of 2 : Report Selection
Select any report from the list of custom reports to proceed. This window shows the list of custom reports available. Click New to create a new custom report. Click Edit to modify the selected report. Click Delete to delete any selected custom report. Select a custom report, and then click View Details to view the list of fields defined for the selected report.
Report Name
Object Category
Description
OU General
Organizational Units
Ou General details.
User Memberof
Users
User Membership details
User Status
Users
User Account Status
New
Edit
Delete
View Details
<Back
Next>
Close

3) ***Select*** a report from the list of reports.

You can *create* a *new* custom report by clicking ***New*** button. This will launch the ***Custom Reports*** *Wizard* which will guide you through the steps for creating a custom report.

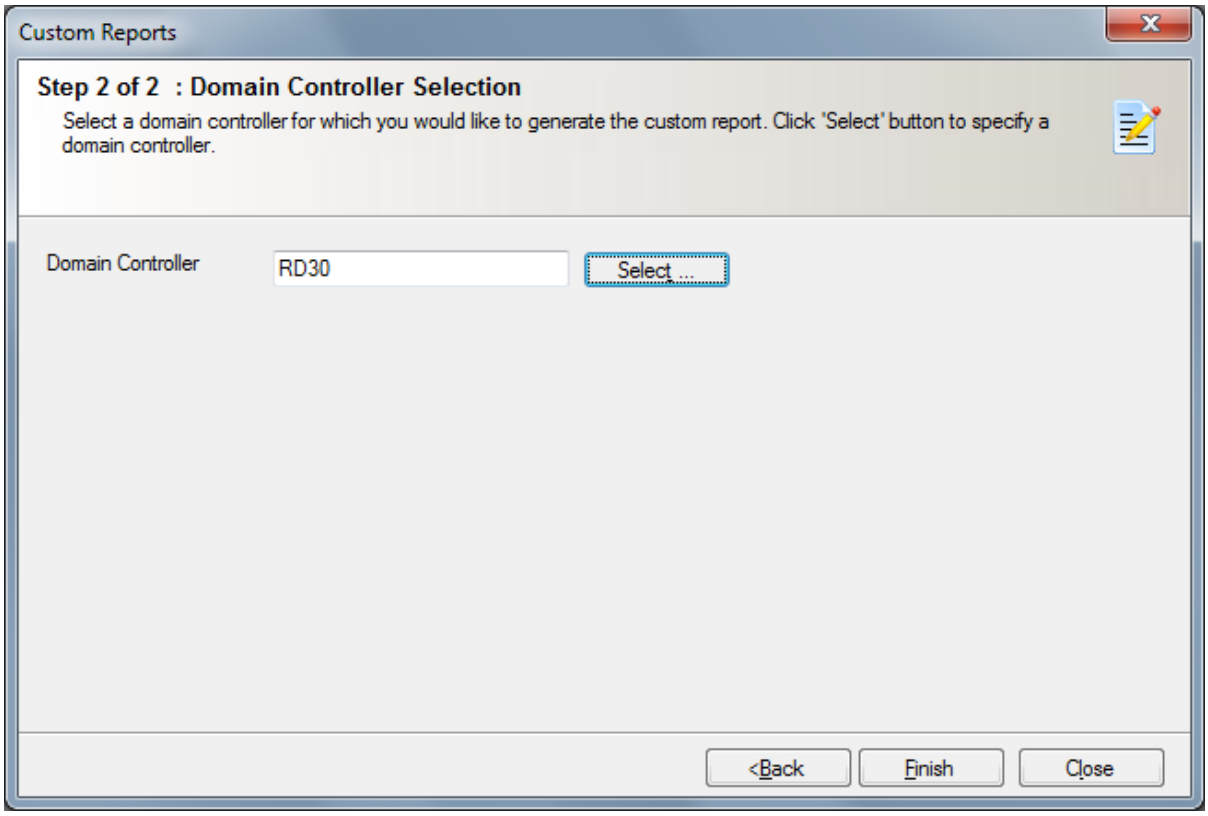
To *modify* an existing custom report, select a report, and then click ***Edit*** button. The ***Custom Reports*** *Wizard* will be displayed which will guide you through the steps for ***editing*** a custom report.

Click ***Delete*** button to *delete* any selected custom report. Please note that you cannot delete a custom report which currently is being viewed.

You can ***view*** the list of fields defined for any selected report by clicking ***View Details*** button.

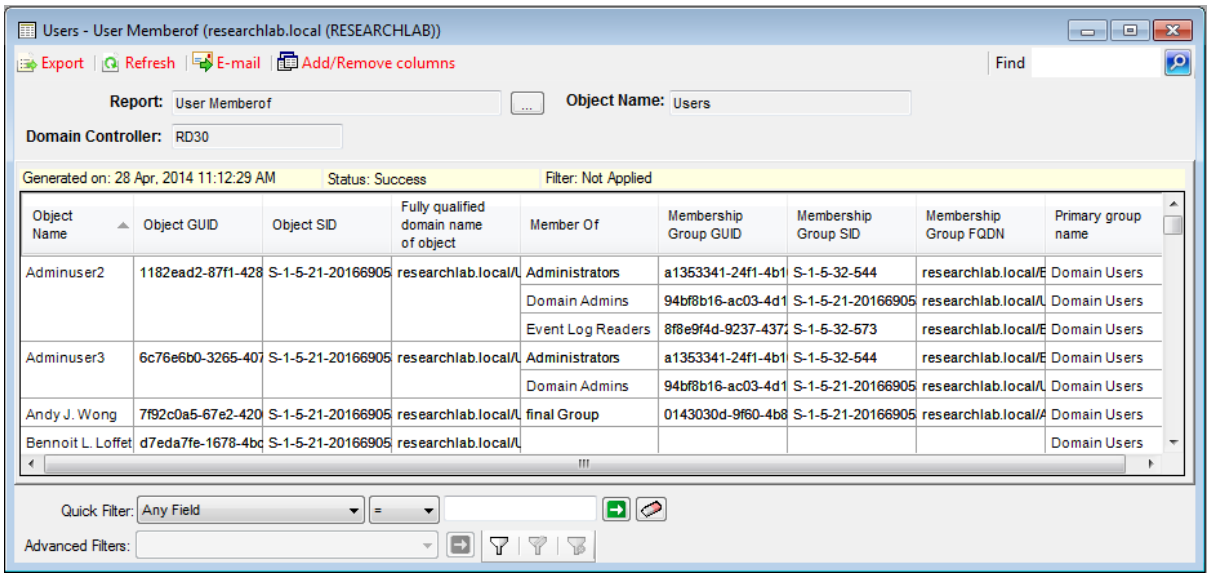
Click ***Next*** to proceed to the next step.

4) **Specify** a ***domain controller*** for which you want to generate the selected custom report. Click ***Select*** button to specify a domain controller. The Connection Manager will be displayed which will allow you to specify a domain controller.


Custom Reports
Step 2 of 2 : Domain Controller Selection
Select a domain controller for which you would like to generate the custom report. Click 'Select' button to specify a domain controller.
Domain Controller
RD30
Select ...
<Back
Finish
Close

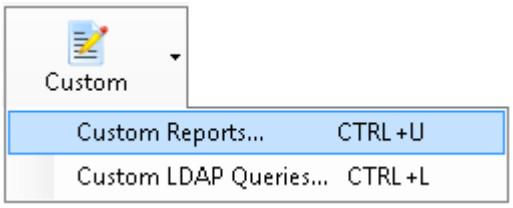
5) Click ***Finish*** to generate the report.

6) After the data collection process is complete, the report would be generated in a report window as shown below:

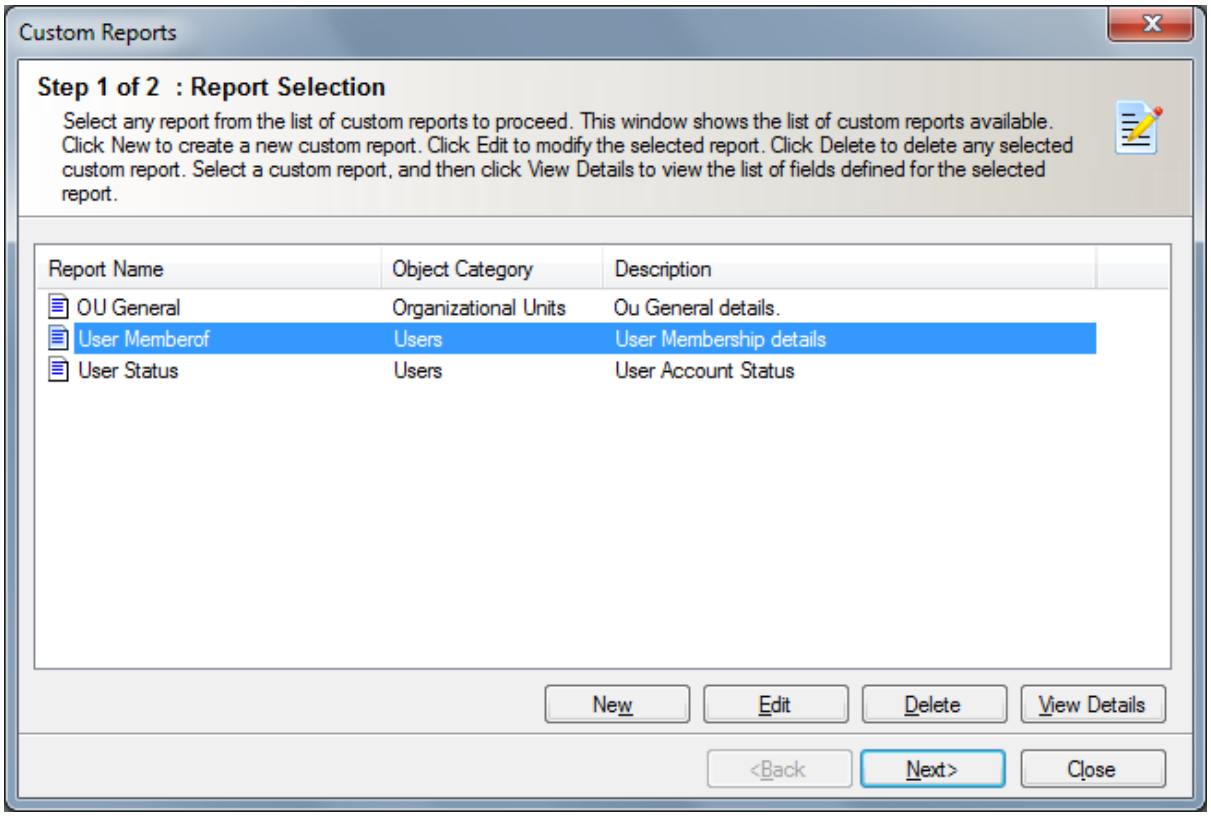


7) To generate another custom report click on the browse button ("...") next to Report name in the report window.

8.4 How to Manage Custom Reports?



Click in the tool bar to launch the ***Custom Reports*** Window. The Custom Reports Window shows the list of custom reports available. The Object Category column shows the name of the object for which a custom report was created.


Custom Reports
Step 1 of 2 : Report Selection
Select any report from the list of custom reports to proceed. This window shows the list of custom reports available. Click New to create a new custom report. Click Edit to modify the selected report. Click Delete to delete any selected custom report. Select a custom report, and then click View Details to view the list of fields defined for the selected report.
Report Name
Object Category
Description
OU General
Organizational Units
Ou General details.
User Memberof
Users
User Membership details
User Status
Users
User Account Status
New
Edit
Delete
View Details
<Back
Next>
Close

The Custom Reports Window allows you to perform the following operations:

- ***Create*** a new Custom Report
- ***Edit*** an existing Custom Report
- ***Delete*** a custom report
- ***View*** fields defined for a custom report
- ***Generate*** a custom report

Create a new Custom Report

1) To ***create*** a new custom report click ***New*** button in the Custom Reports Manager window. The Custom Reports Wizard will appear on the screen.
2) Follow the steps as outlined in How to create Custom Reports?

Edit an existing Custom Report

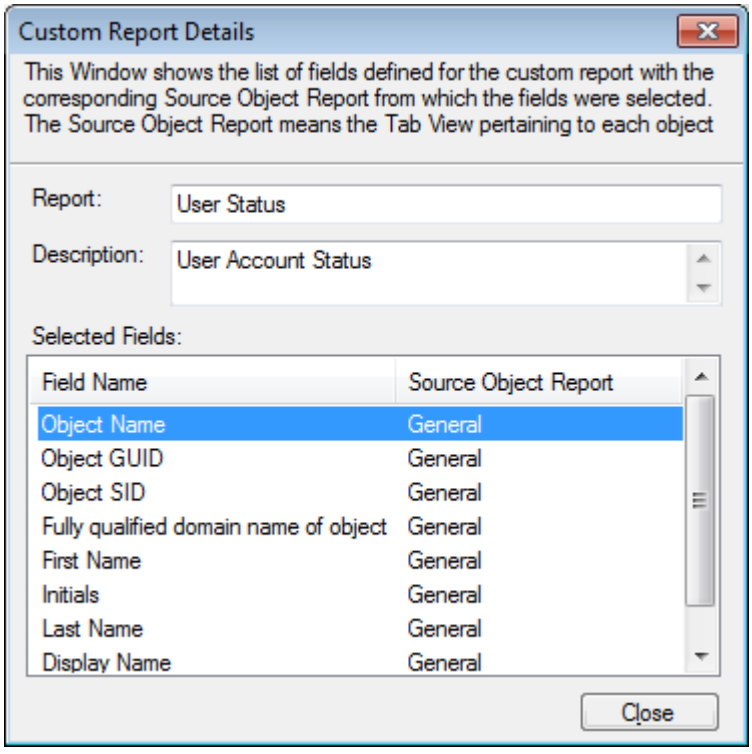
1) To ***edit*** a custom report click ***Edit*** button in the Custom Reports Manager window. The ***Custom Reports*** *Wizard* will appear on the screen which will guide you through the edit operation.
2) During the *edit* operation you can *modify* the list of fields that make up the custom report and the report's description.

Delete a custom report

To ***delete*** a custom report, select the report you want to delete, and then click ***Delete*** button. The selected custom report and all its associated saved filters, if any, will be deleted ***permanently***. Further, the custom report will be removed from scheduled tasks, if any, already scheduled.

View fields defined for a custom report

To view details of a custom report select the report, and then click ***View Details*** button. The selected ***custom report's details*** would be shown as below:



The Details window shows the custom report name, **description** and the list of fields defined for the report. Also, this window shows the Object Report name from which respective fields were selected in the "Source Object Report" column. Object Report means the Tab Views pertaining to each object in the Object Reports window.

Generate a custom report

To generate a custom report follow the steps as outlined in How to generate Custom Reports?

Chapter 9

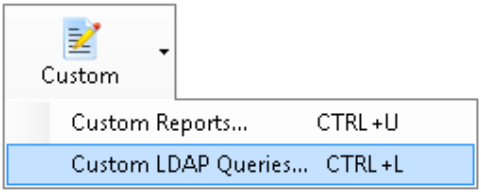
9 Custom LDAP Query Reports

9.1 About Custom LDAP Queries

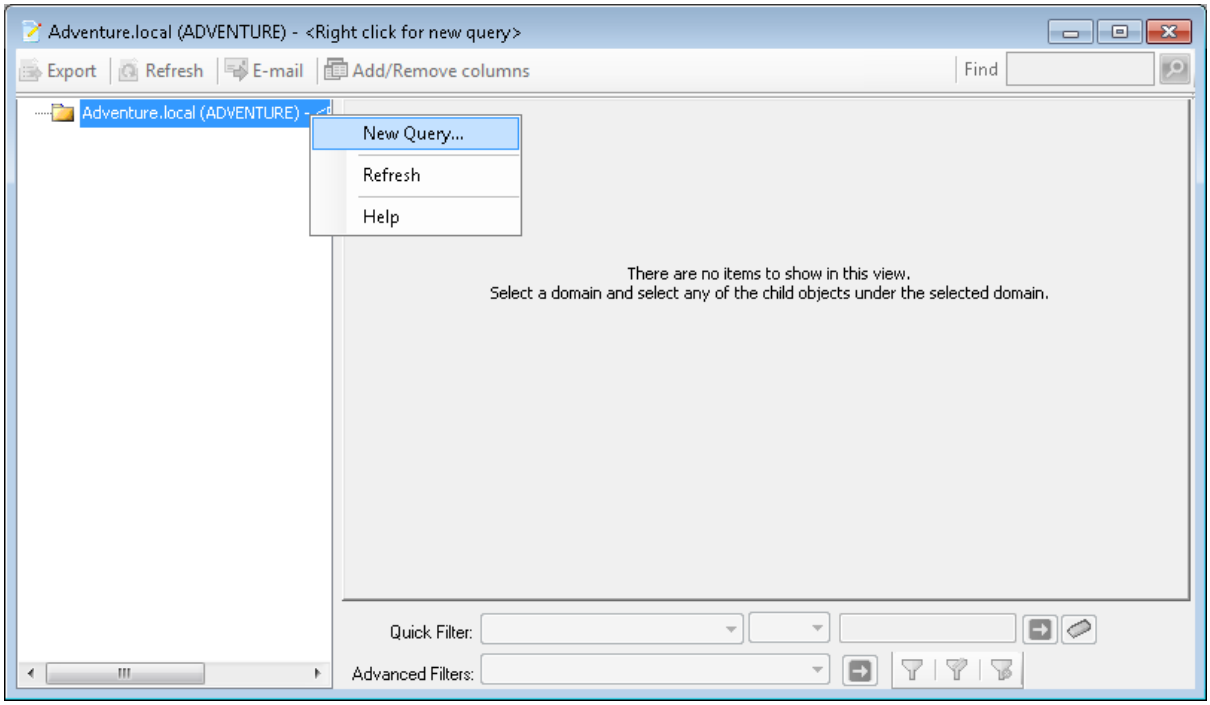
The ***Custom LDAP Queries*** feature in ARKAD allows the user to create their own ***Custom LDAP Query Reports*** to search only the specified domain partition, and searches can be narrowed down to a single container object.

- How to Create Custom LDAP Query Report?
- How to generate Custom LDAP Query Report?
- How to manage Custom LDAP Query Report?
- How to Delete Custom LDAP Query Report?

9.2 How to Create Custom LDAP Query Report?

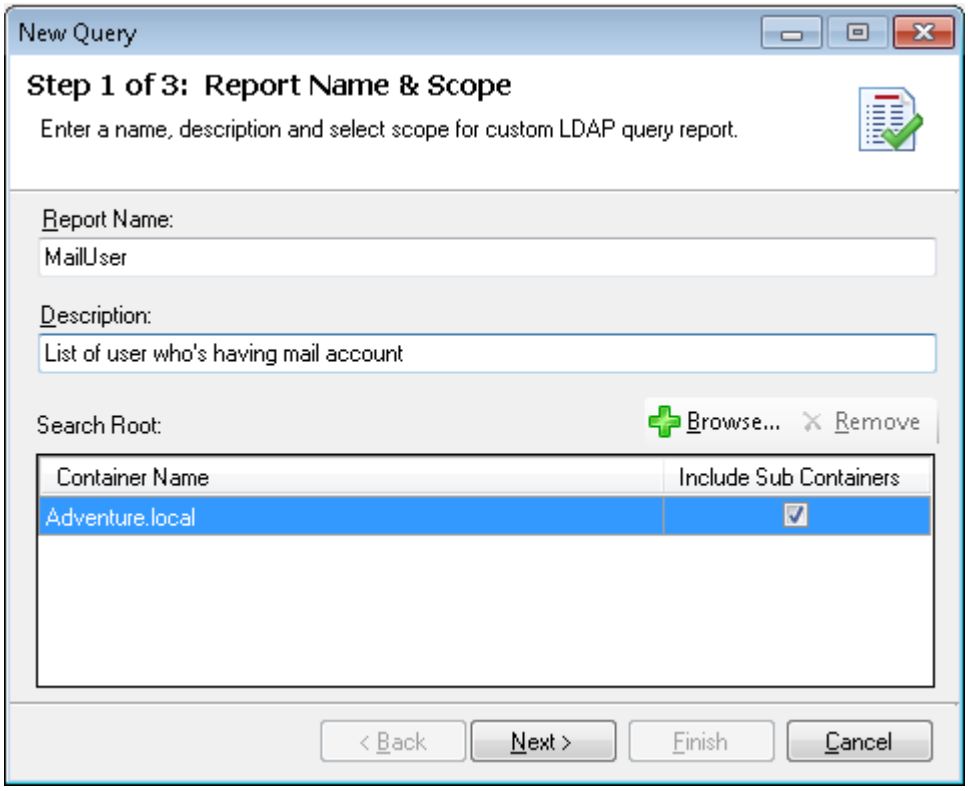
Select 

option under ***Custom*** button. The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.



Right click on domain node in ***Custom LDAP Queries*** window and create a ***New Query.*** The ***New Query*** wizard will be displayed as shown below.

Step 1: Enter Custom LDAP Query Name and container(s)

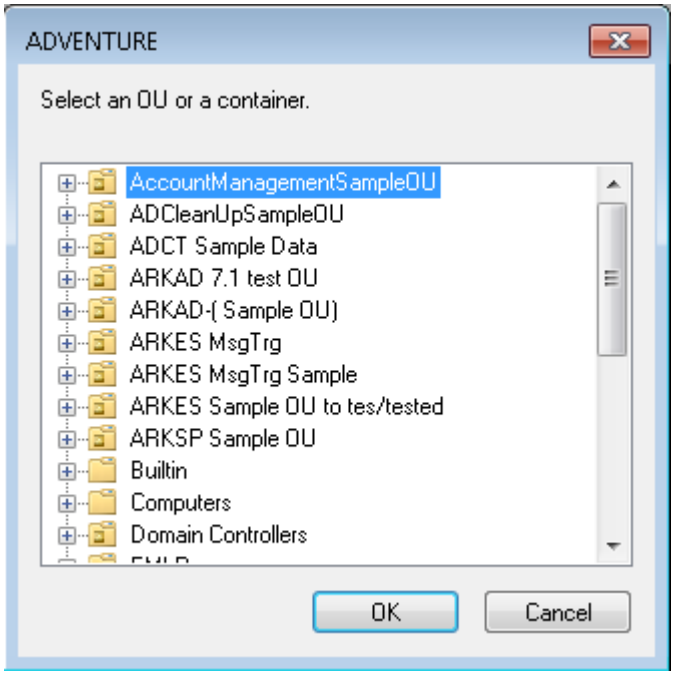


To create a Custom LDAP Query report

1) In ***Name***, type a *query name*.

2) In ***Description***, type a query description.

3) Click ***Browse*** to define the container(s) from which to begin your search.



To search all *subcontainers* of the selected container, select the ***Include subcontainers'*** *check box.*

4) Specify the *Custom LDAP Query.*

The LDAP query is used to perform searches for a specific resource. To conduct your search, enter your search string here. For example, to find a common name in the domain, type **(cn**=name) where name is the name of the object.

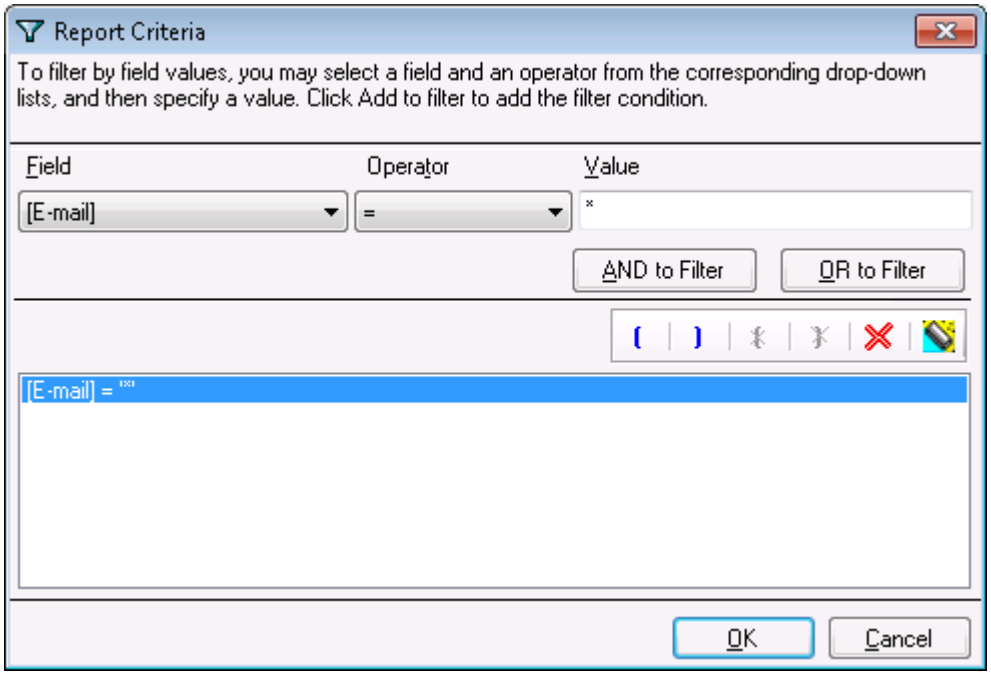
5) Click ***Next*** *t*o Proceed to the Next Step.

Step 2: Object Selection and LDAP query selection (optional)

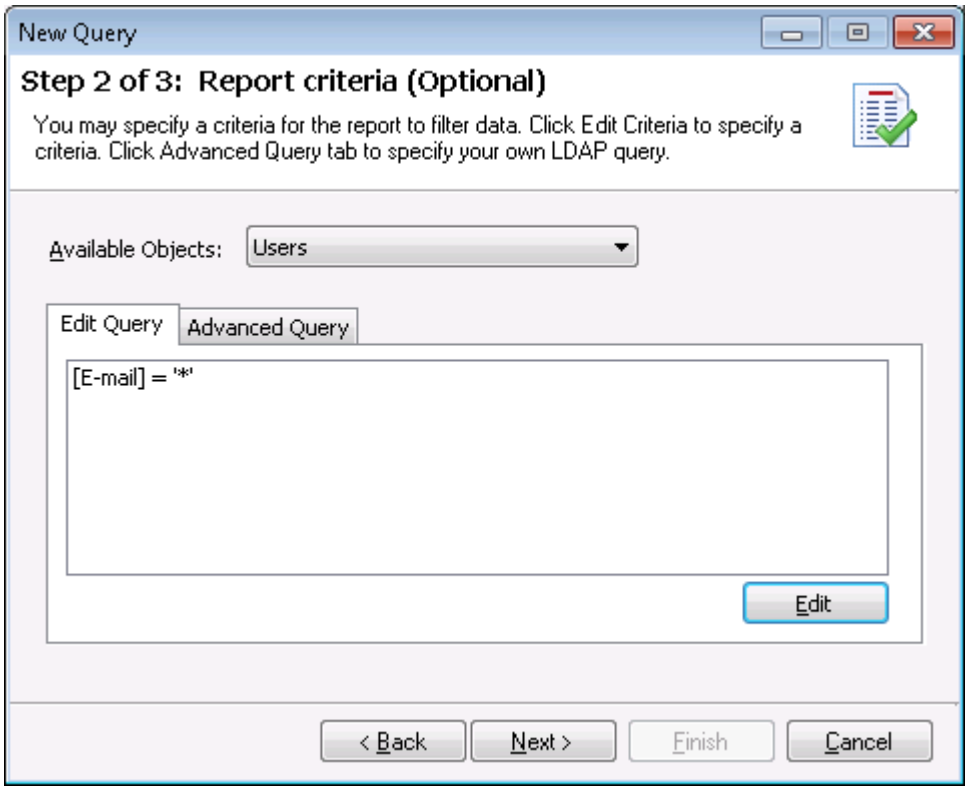
1) Choose ***Object Name*** from available combobox.

2) To specify LDAP query for the report click ***Edit*** button. For advanced LDAP query choose *'Advanced query'* tab.

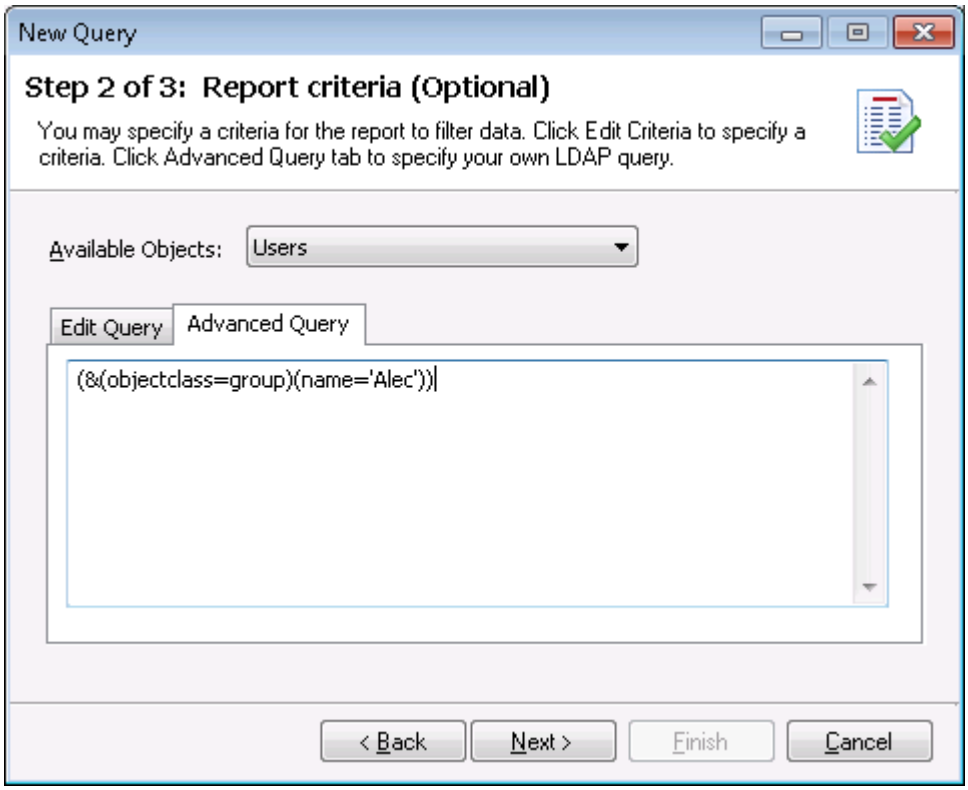
3) The ***Report Criteria*** window shows up on screen. Select a field, an operator specify a ***value*** for the condition. Click Add to Filter button to add the filter condition. The Report Criteria windows is show below:



4) Click ***OK*** to apply the criteria to the report. The applied ***report criteria*** would be displayed as shown below:


New Query
Step 2 of 3: Report criteria (Optional)
You may specify a criteria for the report to filter data. Click Edit Criteria to specify a criteria. Click Advanced Query tab to specify your own LDAP query.
Available Objects:
Users
Edit Query
Advanced Query
[E-mail] = '*'
Edit
< Back
Next >
Finish
Cancel

5) Choose ***Advanced Query*** to enter our manual LDAP queries.


New Query
Step 2 of 3: Report criteria (Optional)
You may specify a criteria for the report to filter data. Click Edit Criteria to specify a criteria. Click Advanced Query tab to specify your own LDAP query.
Available Objects:
Users
Edit Query
Advanced Query
(&(objectclass=group)(name='Alec'))
< Back
Next >
Finish
Cancel

6) Click ***Next*** to Proceed to the Next Step.

Step 3: Field Selection

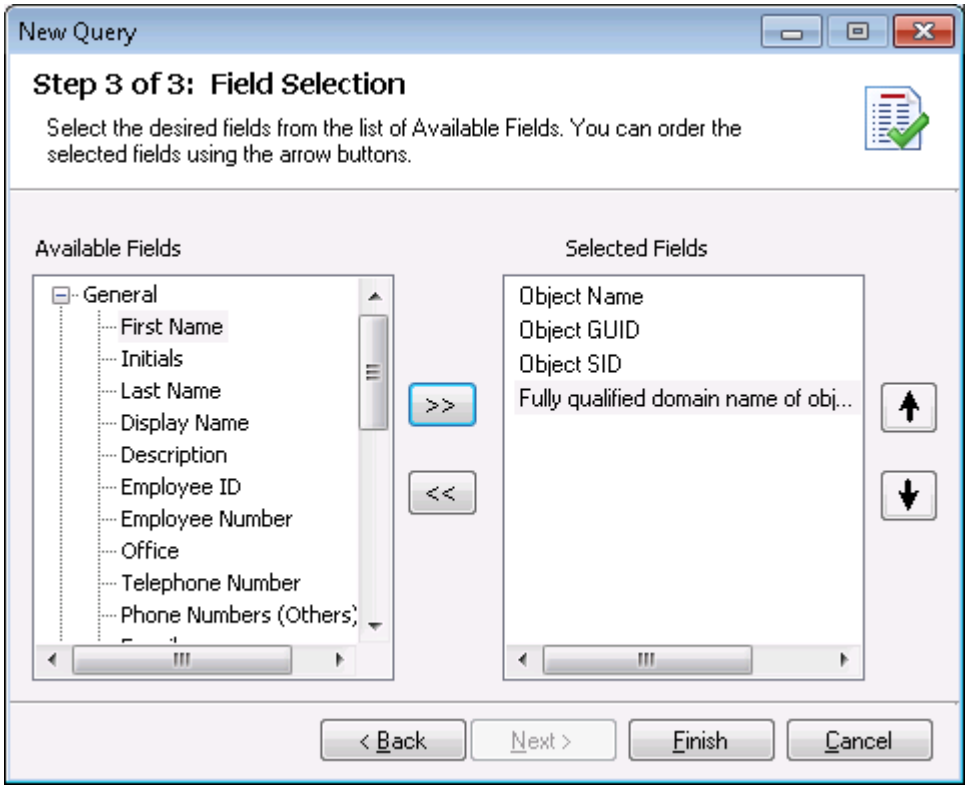
1) To ***select*** fields from a report, click on the desired **field** in the list *of* ***Available Fields,*** *and then click* ***button.***

2) To ***remove selected fields***, click on the desired field in the list of ***Selected Fields,*** and then *click* ***button.***

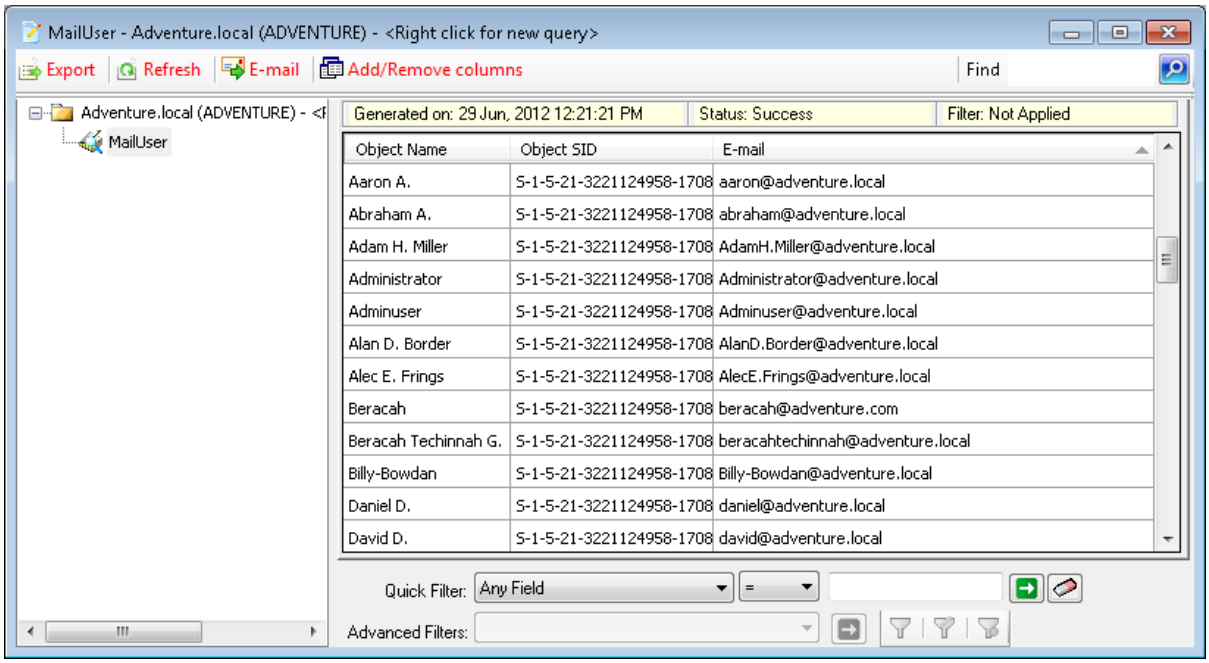
3) You can use the ***arrow*** buttons to **order** the selected fields. To move a ***field up*** by one position in the list of selected fields *click* ***button.*** To move a ***field down*** by one position in the list of selected fields *click* ***button.***

4) To choose fields from another report, select the desired report from the Report Name drop-down list, and then perform the above mentioned steps.

5) Click ***'Finish'*** to save the Custom LDAP Query Report settings

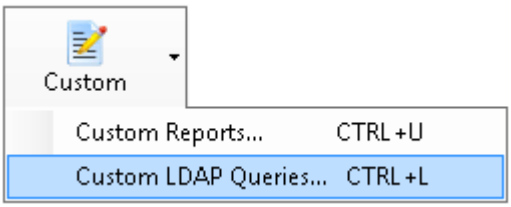


The task will be added to domain node and will be displayed as shown below:



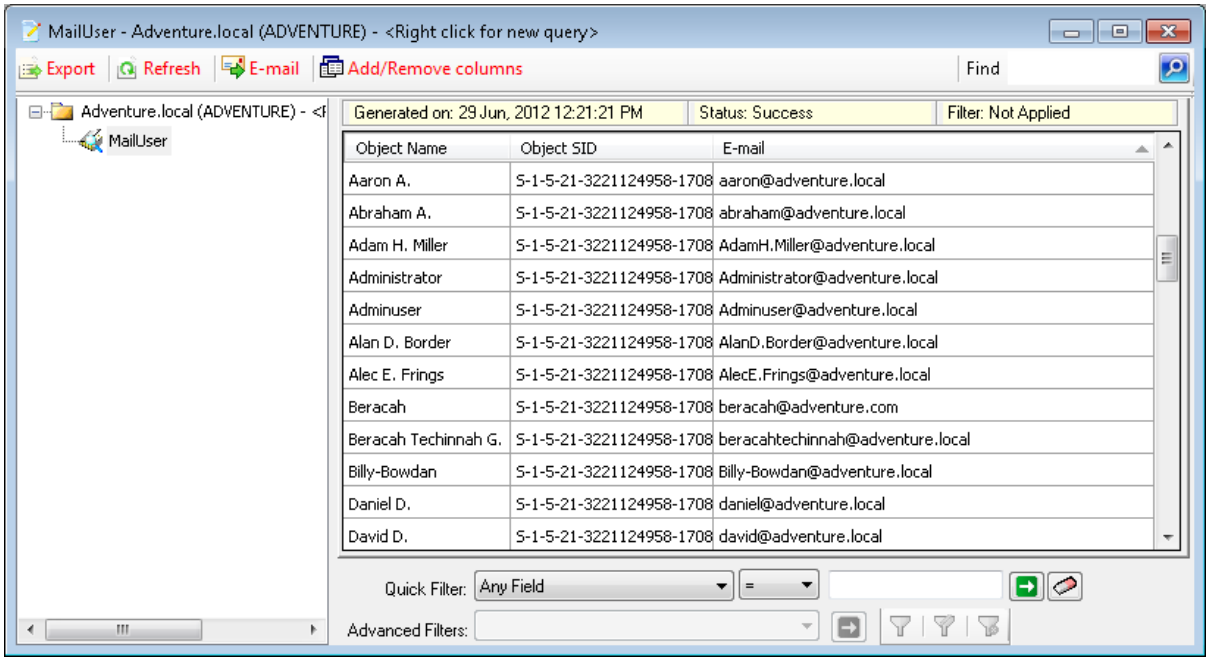
To generate a Custom LDAP Query Report, Refer How to generate Custom LDAP Query Report?

9.3 How to Generate Custom LDAP Query Report?



Select *option* under ***Custom*** button. The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.

This window shows the list of reports that can be generated. Select a report from the **list of reports** under domain node in *Custom LDAP Queries* window. After the data collection process is complete, the report would be generated in a report window as shown below:



9.4 How to Manage Custom LDAP Query Report?

The ***Custom LDAP Queries Reports*** Window allows you to perform the following operations:

- ***Create*** a new Custom LDAP Query Report
- ***Edit*** an existing Custom LDAP Query Report
- ***Delete*** a Custom LDAP Query Report
- ***Rename*** Custom LDAP Query Report
- ***Generate*** a Custom LDAP Query Report

Create a new Custom LDAP Query Report

1) To ***create*** a new Custom LDAP Query Report click ***New*** button on the domain node in *Custom LDAP Queries* window. The Custom LDAP Query Reports Wizard will appear on the screen.
2) Follow the steps as outlined in How to create Custom LDAP Query Report?

Edit an existing Custom LDAP Query Report

1) To *edit* a Custom LDAP Query Report click ***Edit*** button in the Custom LDAP Queries Reports Manager window. The Custom LDAP Query Reports Wizard will appear on the screen which will guide you through the edit operation.
2) During the edit operation you can modify the list of fields that make up the Custom LDAP Query Report and the report's description.

Delete a Custom LDAP Query Report

To *delete* a Custom LDAP Query Report, select the report you want to delete, and then click ***Delete*** menu. The selected Custom LDAP Query Report and all its associated saved filters, if any, will be deleted *permanently*. Further, the Custom LDAP Query Report will be ***removed*** from scheduled tasks, if any, already scheduled.

Rename a Custom LDAP Query Report

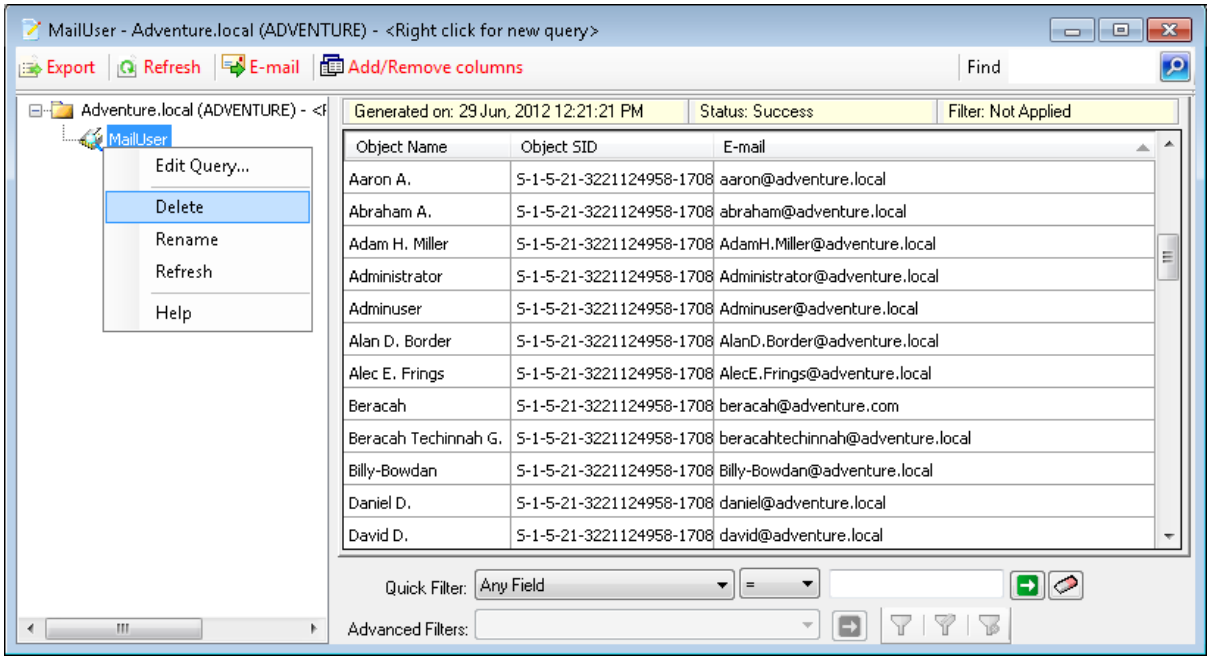
To *rename* a *Custom LDAP Query Report*, ***select*** the *report*, and then click ***Rename*** menu.

Generate a Custom LDAP Query Report

To ***generate*** a Custom LDAP Query Report follow the steps as outlined in How to generate Custom LDAP Query Report?

9.5 How to Delete Custom LDAP Query Report?

Right click on a *Custom LDAP Queries report* node in which you want to *delete* and select ***Delete*** as shown below.



Chapter 10

10 AD Summary Reports

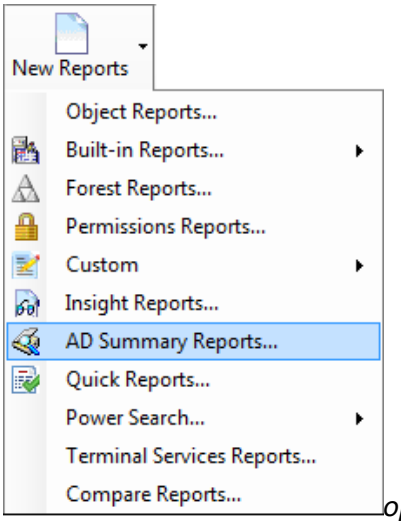
10.1 About AD Summary Reports

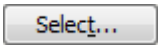
The ***AD Summary reports*** feature provides overall summary information about a single Active Directory domain. For example, total no of users, Groups, Computers in a Domain / Organizational Units. AD Summary reports are easy to use and speeds-up the report generation process.

The AD Summary tool currently reports on the following objects:

- Domain
- Organizational Units
- Computer Accounts
- Users

10.2 How to generate AD Summary Reports?



Select *option* under *New Report* button. The report window will be launched. Click on 

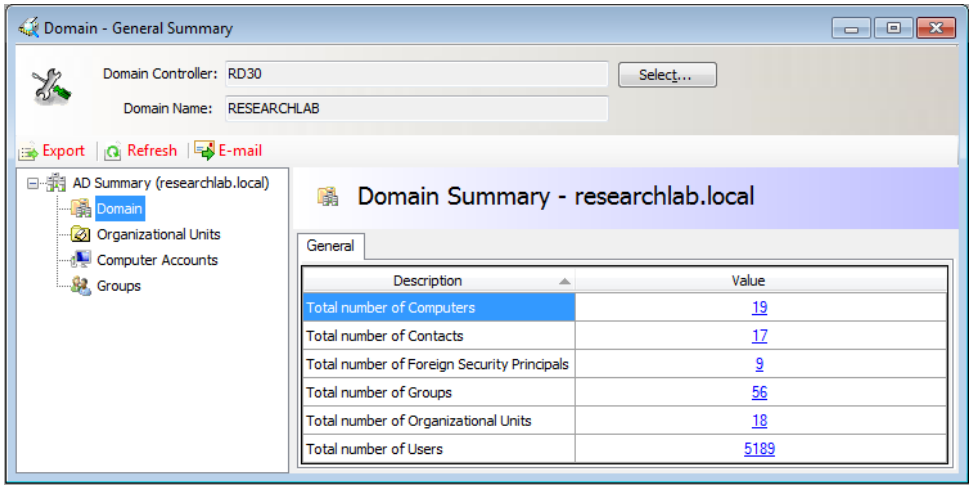
button, the Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller.

The report window will be enabled after the domain and the selected domain controller are validated. Select and expand the root node in the left pane of the newly launched report window.

Domain General Summary report

Click on ***'Domain'*** node in the left pane to view the following information: **{Total no of Users, Groups, Computers, Organizational Units, Contacts, Foreign Security Principals in an Active Directory domain}.**

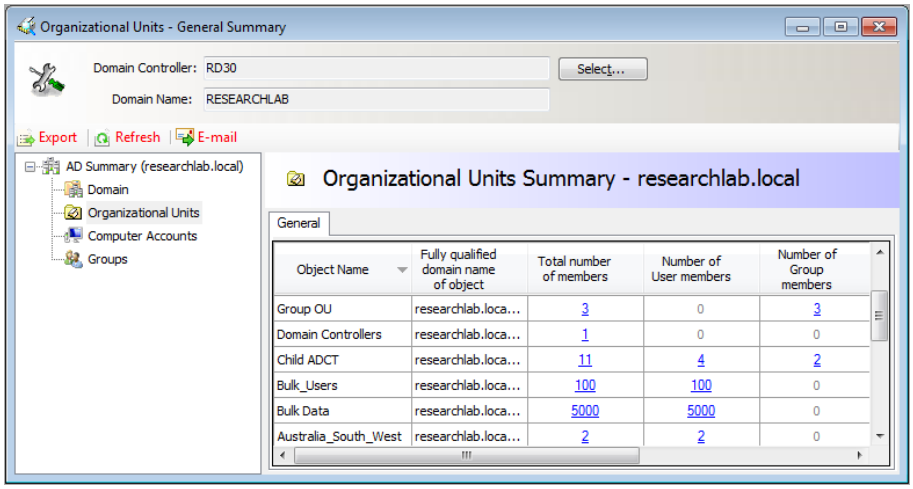
The output would be displayed as shown below:



Organizational Units General Summary report

Click on ***'Organizational Units'*** node in the left pane to view the following information: **{Total no of members, No of User members, No of Group members, No of OU members, No of Computer members, No of Contact members}.**

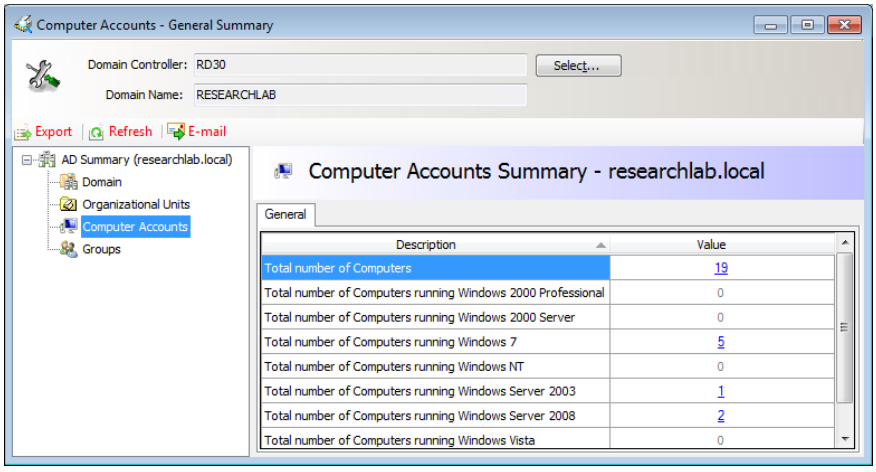
The output would be displayed as shown below:



Computer Accounts General Summary report

Click on ***'Computer Accounts'*** node in the left pane to view the following information: ***{Total no of Computers, Total no of Computers running Windows XP Professional, Total no of Computers running Windows Server 2003, Total no of Computers running Windows Vista, Total no of Computers running Windows Server 2008, Total no of Computers running Windows NT, and Total no of Computers running Windows 7}.***

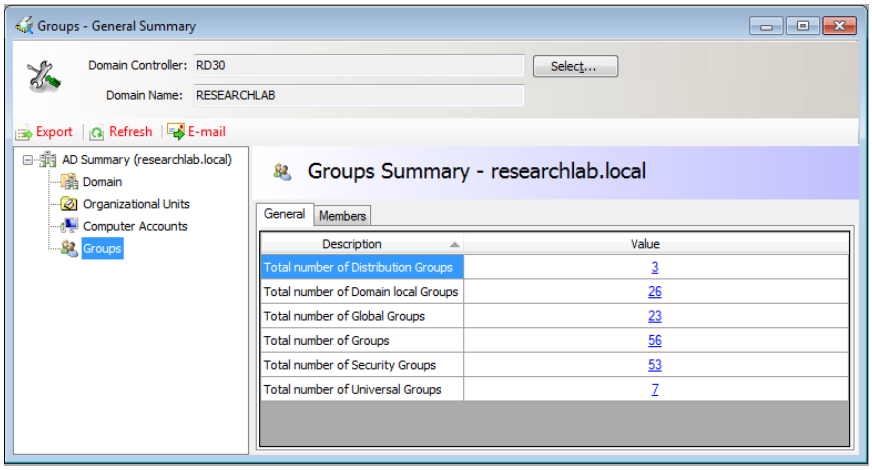
The output would be displayed as shown below:


Computer Accounts - General Summary
Domain Controller: RD30
Select...
Domain Name: RESEARCHLAB
Export
Refresh
E-mail
AD Summary (researchlab.local)
Domain
Organizational Units
Computer Accounts
Groups
Computer Accounts Summary - researchlab.local
General
Description
Value
Total number of Computers 19
Total number of Computers running Windows 2000 Professional 0
Total number of Computers running Windows 2000 Server 0
Total number of Computers running Windows 7 5
Total number of Computers running Windows NT 0
Total number of Computers running Windows Server 2003 1
Total number of Computers running Windows Server 2008 2
Total number of Computers running Windows Vista 0

Groups General Summary report

Click on ***'Groups'*** node in the left pane and select ***'General'*** tab to view the following information: **{Total no of Groups, Total no of Security Groups, Total no of Distribution Groups, Total no of Domain local Groups, Total no of Universal Groups, Total no of Global Groups}.**

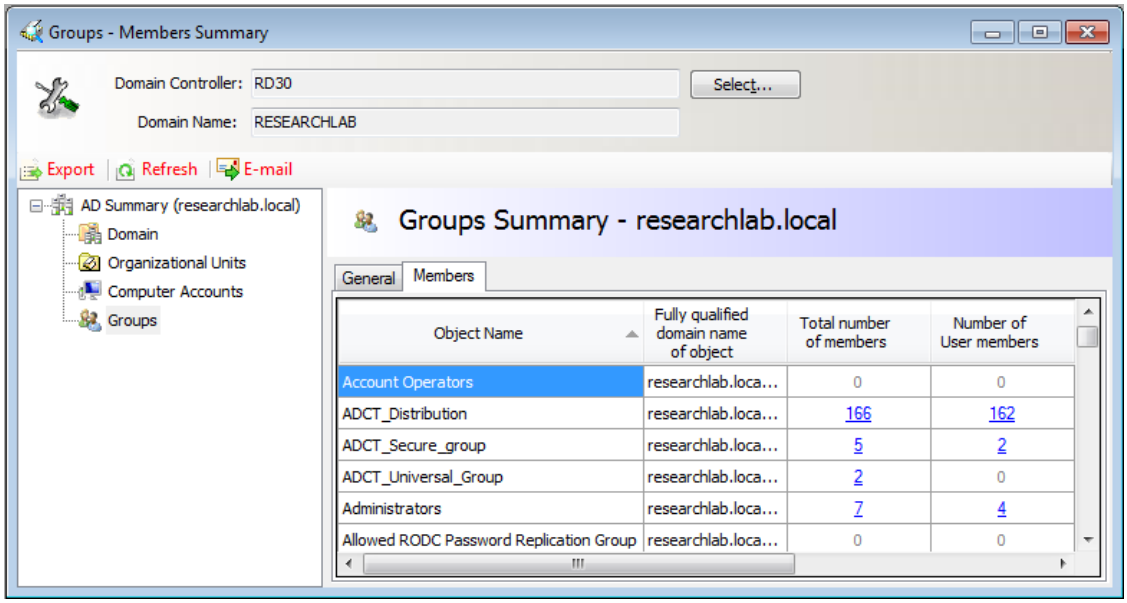
The output would be displayed as shown below:



Group Members Summary report

Click on ***'Groups'*** node in the left pane and select ***'Members'*** tab to view the following information: **{Total no of members, No of User members, No of Group members, No of Computer members, No of Contact members}.**

The output would be displayed as shown below:



Chapter 11

11 Insight Reports

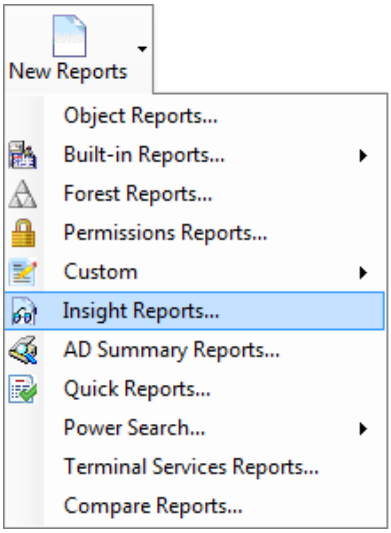
11.1 About Insight Reports

The *Insight* tool in ARKAD reports Summary and Detailed information based on "frequency of occurrence (Counts)" of objects and their attributes, for example, "Number of recently created objects in a given time period". Some of the reported items in the Summary are based on certain parameters (Count, Date etc.) that may be modified to get the desired report. The reports provide an ***"Insight"*** into Active Directory by producing some meaningful statistics on certain important objects in Active Directory.

The Insight tool currently reports on the following objects:

- **Organizational Units**
- **Computer Accounts**
- **Users**
- **Groups**

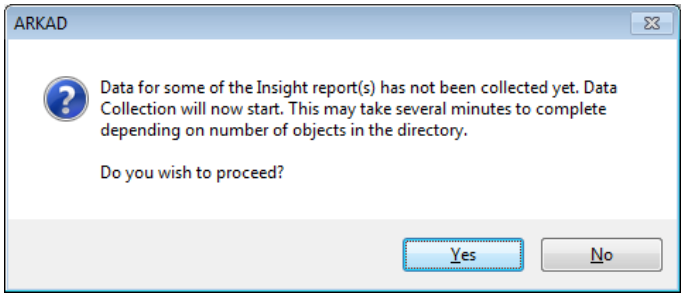
11.2 How to view Insight Report for Organizational Units?

Click *on* 

button. The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click on ***Organizational Units.***

The following message will appear on screen, if the report data has not been already collected:


ARKAD
Data for some of the Insight report(s) has not been collected yet. Data Collection will now start. This may take several minutes to complete depending on number of objects in the directory.
Do you wish to proceed?
Yes
No

Select ***Yes*** to collect data.

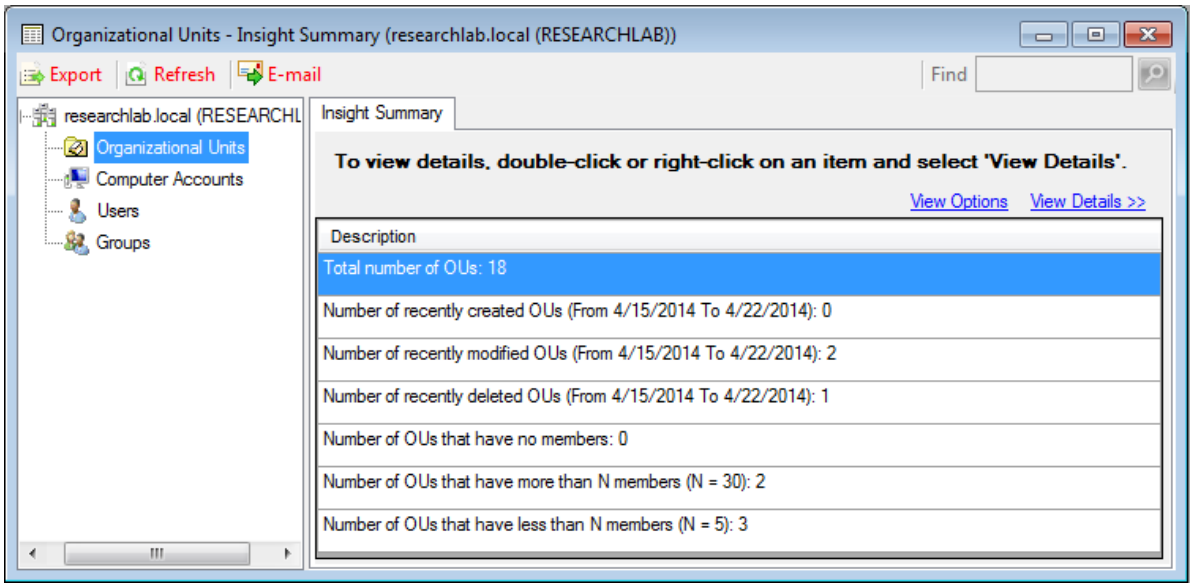
NOTE:

- The ***Insight report*** items of an object depend on data from its corresponding "Object Report" tab(s). For instance, the item that displays the count of objects created in a certain time period depends on data from the "Object" tab. So, when the data collection begins, data for all the "Object Report" tab(s) would be collected first, after which the Insight report would be generated.
- If you select **No,** then the required "Object Report(s)" data would not be collected. As a result, you may see zeroes against Insight items for which data is

not available. However, note that, you may select **No** when you refresh Insight report data. In that case the existing report data will remain unchanged.

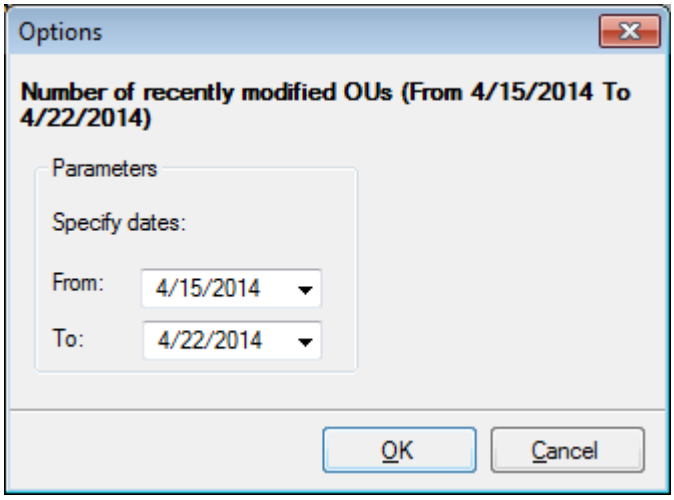
- Also, note that the same message would be displayed when you click ***Refresh Data*** on the tool bar.

The report would be displayed as shown below:


Organizational Units - Insight Summary (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Find
researchlab.local (RESEARCHL
Organizational Units
Computer Accounts
Users
Groups
Insight Summary
To view details, double-click or right-click on an item and select 'View Details'.
View Options
View Details >>
Description
Total number of OUs: 18
Number of recently created OUs (From 4/15/2014 To 4/22/2014): 0
Number of recently modified OUs (From 4/15/2014 To 4/22/2014): 2
Number of recently deleted OUs (From 4/15/2014 To 4/22/2014): 1
Number of OUs that have no members: 0
Number of OUs that have more than N members (N = 30): 2
Number of OUs that have less than N members (N = 5): 3

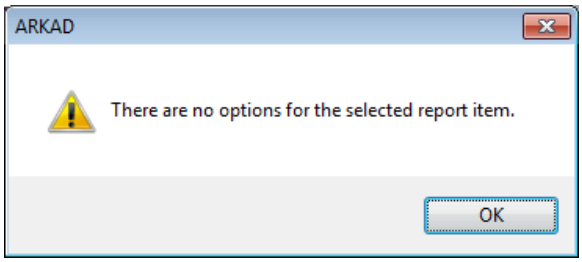
View Options

You can modify parameters of the selected item by clicking on ***View Options*** and get the desired report. The **Options** dialog would be displayed as shown below:



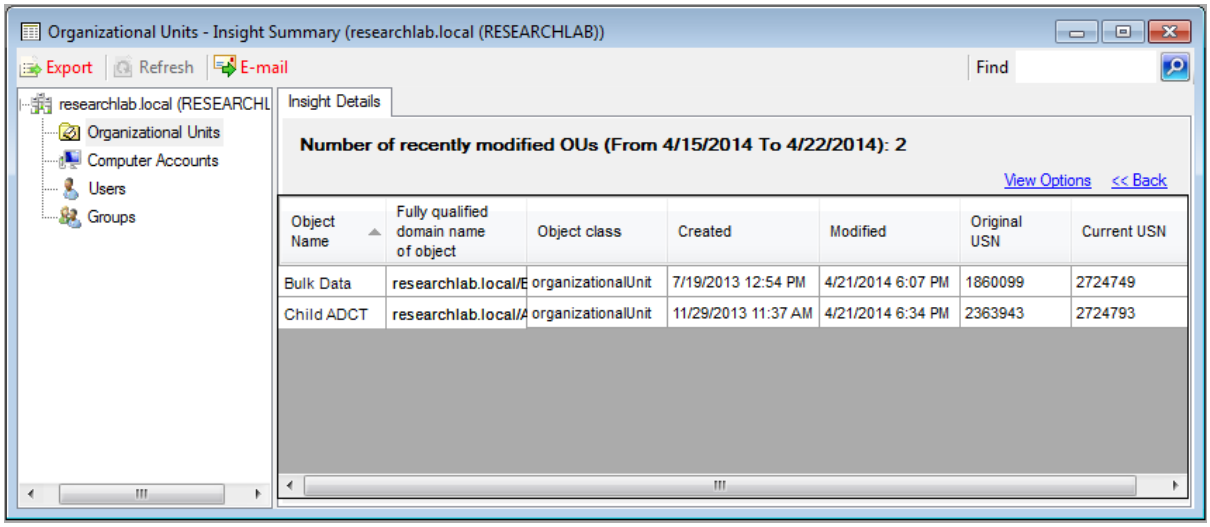
Modify the *parameters* and *click* ***OK*** to refresh the report. Note that parameters can be set both in "Summary" and "Details" view of Insight report. Furthermore, parameters can be set on an item-by-item basis only.

NOTE: Some of the reported items may not have parameters to set. If the selected item does not have parameters, then you would see the following message appear on screen:



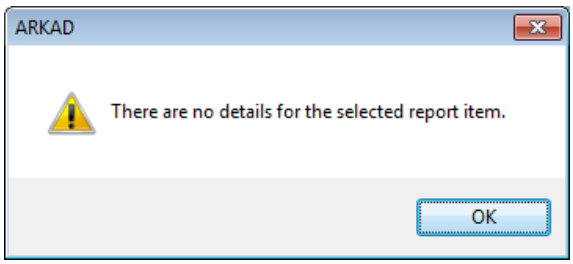
View Details

You can view detailed information of the selected item, by clicking ***View Details*****.** Details of the selected item would be displayed as shown below:



To navigate back to the "Summary" view of the Insight report click ***Back.***

NOTE: Some of the reported items may not have any details, for instance, the item that displays the total count of objects. If the selected item does not have details associated with it, then you would see the following message appear on screen:

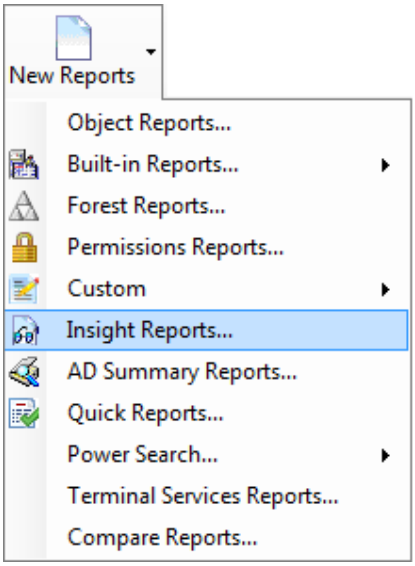


Items Reported

The following table lists the *count-based items* for ***Organizational Units*** and their corresponding settings:

Count-based Item Name	Description	Parameters	Detail Report
Total number of OUs	Displays the total count of OUs in the domain.	None	No detail report
Number of recently created OUs	Displays the count of OUs that were created in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Organizational Units.
Number of recently modified OUs	Displays the count of OUs that were modified in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Organizational Units.
Number of recently deleted OUs	Displays the count of OUs that were deleted in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Deleted Objects" report for Organizational Units.
Number of OUs that have no members	Displays the count of OUs that are empty.	None	Displays the "Object" report for Organizational Units.
Number of OUs that have more than N members	Displays the count of OUs that have more than the specified number of members.	Specify a number (count) of members.	Displays "Members" report for Organizational Units.
Number of OUs that have less than N members	Displays the count of OUs that have number of members less than the specified number.	Specify a number (count) of members.	Displays "Members" report for Organizational Units.

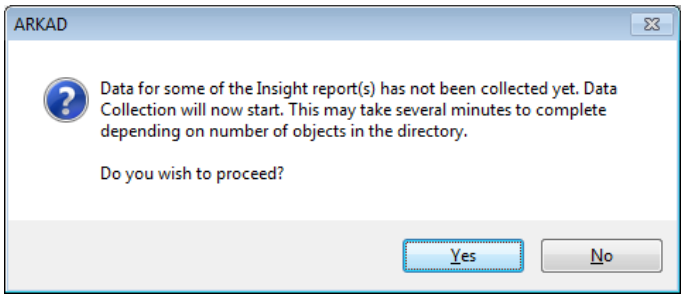
11.3 How to view Insight Report for Computer Accounts?

Click *on* 

button. The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click on **Computer Accounts.**

The following message will appear on screen, if the report data has not been already collected:


ARKAD
Data for some of the Insight report(s) has not been collected yet. Data Collection will now start. This may take several minutes to complete depending on number of objects in the directory.
Do you wish to proceed?
Yes
No

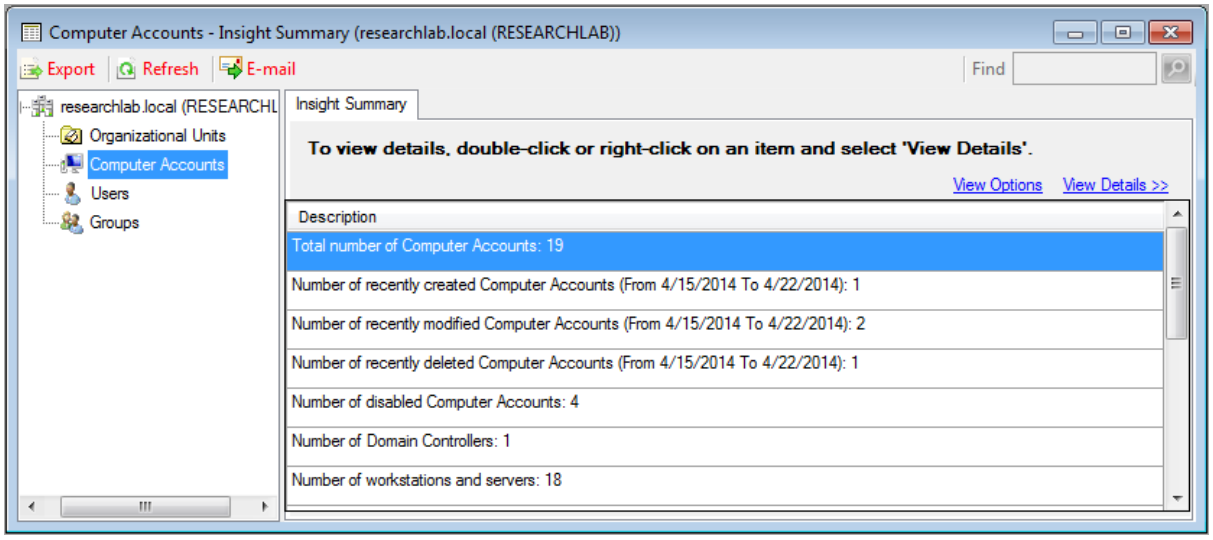
Select ***"Yes"*** to collect data.

NOTE:

- The Insight report items of an object depend on data from its corresponding "Object Report" tab(s). For instance, the item that displays the count of objects created in a certain time period depends on data from the "Object" tab. So, when the data collection begins, data for all the "Object Report" tab(s) would be collected first, after which the Insight report would be generated.
- If you select **No**, then the required "Object Report(s)" data would not be collected. As a result, you may see zeroes against Insight items for which data is not available. However, note that, you may select **No** when you refresh Insight report data. In that case the existing report data will remain unchanged.

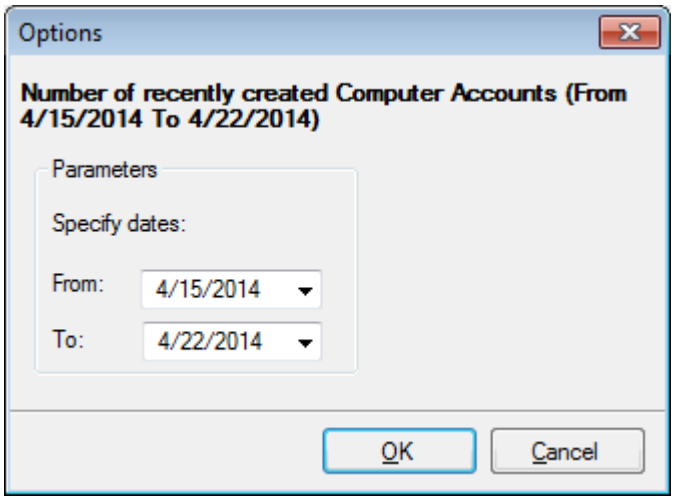
- Also, note that the same message would be displayed when you click **Refresh Data** on the tool bar.

The report would be displayed as shown below:


Computer Accounts - Insight Summary (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Find
researchlab.local (RESEARCHL
Organizational Units
Computer Accounts
Users
Groups
Insight Summary
To view details, double-click or right-click on an item and select 'View Details'.
View Options
View Details >>
Description
Total number of Computer Accounts: 19
Number of recently created Computer Accounts (From 4/15/2014 To 4/22/2014): 1
Number of recently modified Computer Accounts (From 4/15/2014 To 4/22/2014): 2
Number of recently deleted Computer Accounts (From 4/15/2014 To 4/22/2014): 1
Number of disabled Computer Accounts: 4
Number of Domain Controllers: 1
Number of workstations and servers: 18

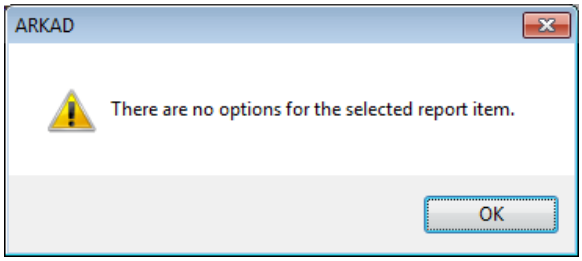
View Options

You can modify parameters of the selected item by clicking on *View Options* and get the desired report. The ***Options*** dialog would be displayed as shown below:



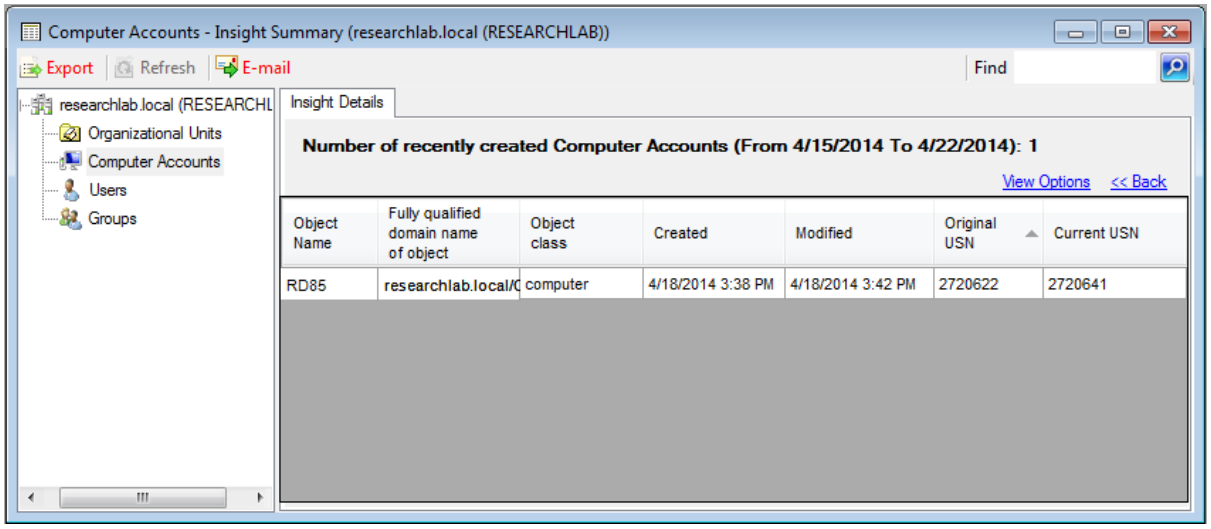
Modify the *parameters* and click ***OK*** to refresh the report. Note that parameters can be set both in "Summary" and "Details" view of Insight report. Furthermore, parameters can be set on an item-by-item basis only.

NOTE: Some of the reported items may not have parameters to set. If the selected item does not have parameters, then you would see the following message appear on screen:



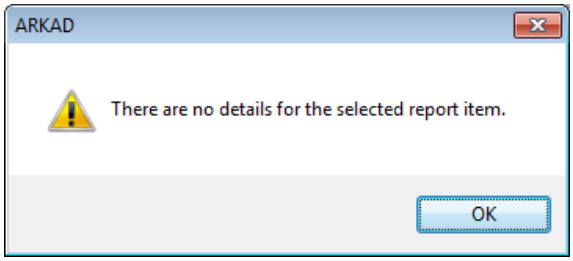
View Details

You can view detailed information of the selected item, by clicking ***View Details***. Details of the selected item would be displayed as shown below:



To navigate back to the "Summary" view of the Insight report click **Back.**

NOTE: Some of the reported items may not have any details, for instance, the item that displays the total count of objects. If the selected item does not have details associated with it, then you would see the following message appear on screen:



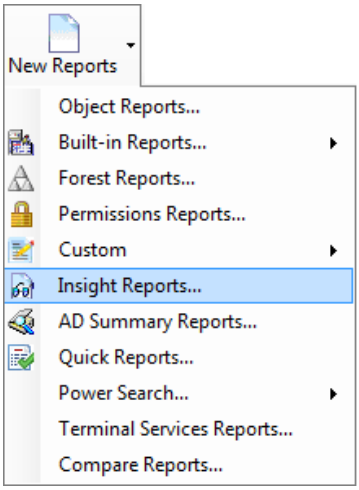
Items Reported

The following table lists the count-based items for ***Computer Accounts*** and their corresponding settings:

Count-based Item Name	Description	Parameters	Detail Report
Total Number of Computers	Displays the total count of Computers in the domain	None	No detail report
Number of recently created computers	Displays the count of computers that were created in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Computer Accounts.
Number of recently modified computers	Displays the count of computers that were modified in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Computer Accounts.
Number of recently deleted computers	Displays the count of computers that were deleted in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Deleted Objects" report for Computer Accounts.
Number of disabled Computers	Displays the count of disabled computer accounts.	None	Displays the "General" report for Computer Accounts
Number of Domain Controllers	Displays the count of domain controllers.	None	Displays the "General" report for Computer Accounts.
Number of workstations and servers	Displays the count of both workstations and servers.	None	Displays the "General" report for Computer Accounts.
Number of computers trusted for delegation	Displays the count of computer accounts trusted for delegation.	None	Displays the "General" report for Computer Accounts.
Number of computers running Windows	Displays the count of computer accounts running	None	Displays the "Operating System" report for

Server 2008	Windows Server 2008.		Computer Accounts.
Number of computers running Windows Vista	Displays the count of computer accounts running Windows Vista.	None	Displays the "Operating System" report for Computer Accounts.
Number of computers running Windows Server 2003	Displays the count of computer accounts running Windows Server 2003.	None	Displays the "Operating System" report for Computer Accounts.
Number of computers running Windows XP Professional	Displays the count of computer accounts running Windows XP Professional.	None	Displays the "Operating System" report for Computer Accounts.
Number of computers running Windows 2000 Server	Displays the count of computer accounts running Windows 2000 Server.	None	Displays the "Operating System" report for Computer Accounts.
Number of computers running Windows 2000 Professional	Displays the count of computer accounts running Windows 2000 Professional.	None	Displays the "Operating System" report for Computer Accounts.
Number of computers running Windows NT	Displays the count of computer accounts running Windows NT.	None	Displays the "Operating System" report for Computer Accounts.

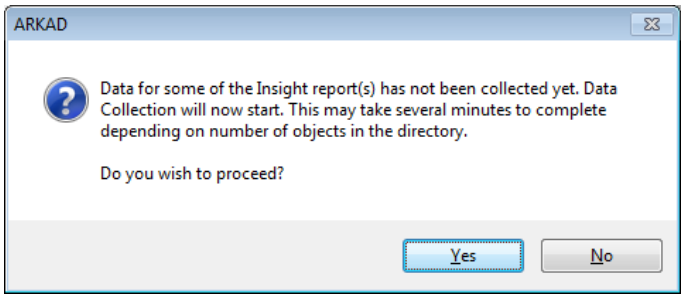
11.4 How to view Insight Report for Users?



Click *on* *button.* The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click on ***Users.***

The following message will appear on screen, if the report data has not been already collected:


ARKAD
Data for some of the Insight report(s) has not been collected yet. Data Collection will now start. This may take several minutes to complete depending on number of objects in the directory.
Do you wish to proceed?
Yes
No

Select ***Yes*** *to* ***collect data.***

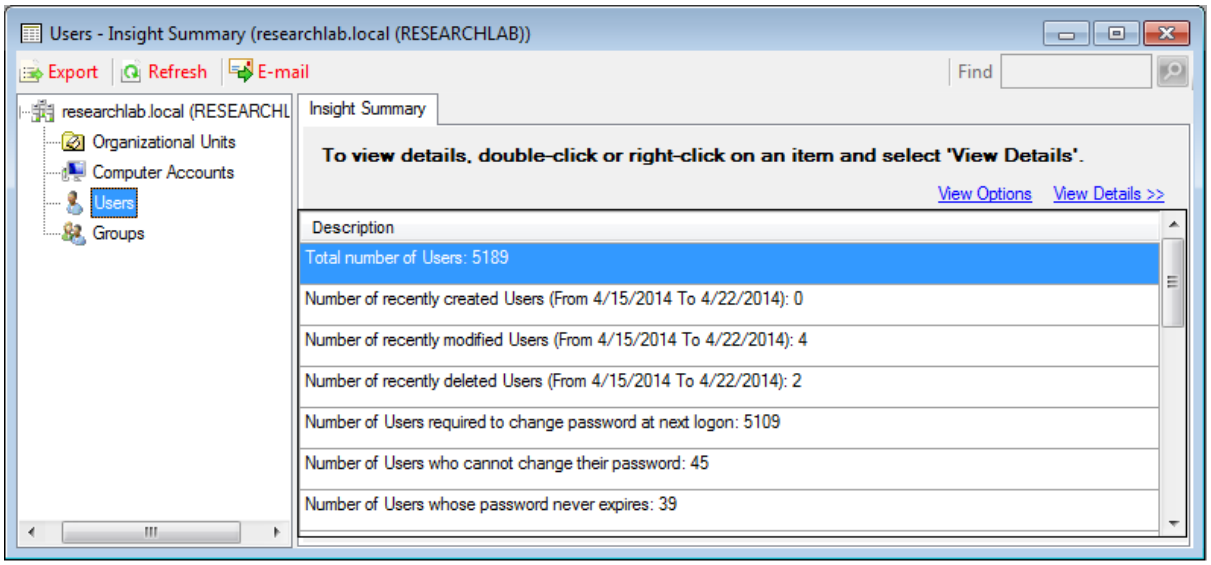
NOTE:

- The Insight report items of an object depend on data from its corresponding "Object Report" tab(s). For instance, the item that displays the count of objects created in a certain time period depends on data from the "Object" tab. So, when the data collection begins, data for all the "Object Report" tab(s) would be collected first, after which the Insight report would be generated.
- If you select **No**, then the required "Object Report(s)" data would not be collected. As a result, you may see zeroes against Insight items for which data is

not available. However, note that, you may select **No** when you refresh Insight report data. In that case the existing report data will remain unchanged.

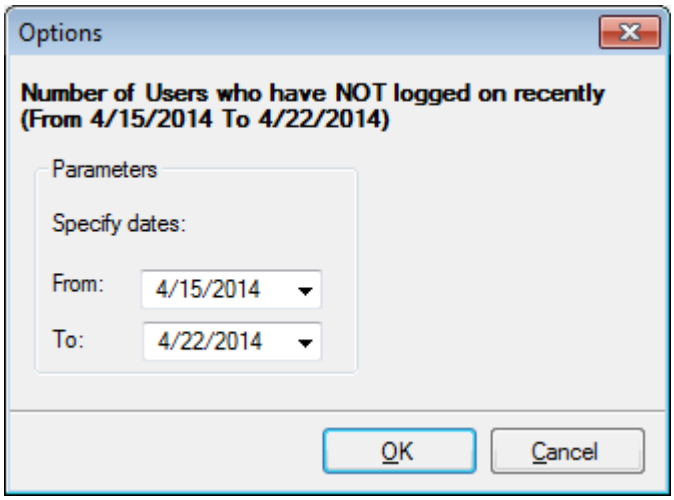
- Also, note that the same message would be displayed when you click *Refresh Data* on the tool bar.

The report would be displayed as shown below:


Users - Insight Summary (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Find
researchlab.local (RESEARCHL
Organizational Units
Computer Accounts
Users
Groups
Insight Summary
To view details, double-click or right-click on an item and select 'View Details'.
View Options
View Details >>
Description
Total number of Users: 5189
Number of recently created Users (From 4/15/2014 To 4/22/2014): 0
Number of recently modified Users (From 4/15/2014 To 4/22/2014): 4
Number of recently deleted Users (From 4/15/2014 To 4/22/2014): 2
Number of Users required to change password at next logon: 5109
Number of Users who cannot change their password: 45
Number of Users whose password never expires: 39

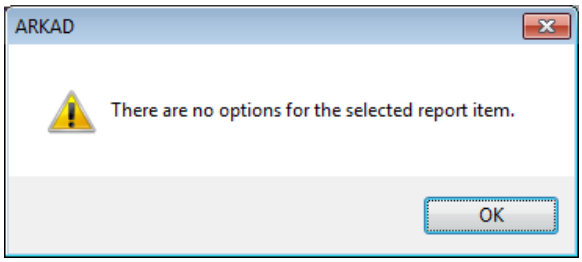
View Options

You can modify parameters of the selected item by clicking on ***View Options*** and get the desired report. The ***Options*** dialog would be displayed as shown below:



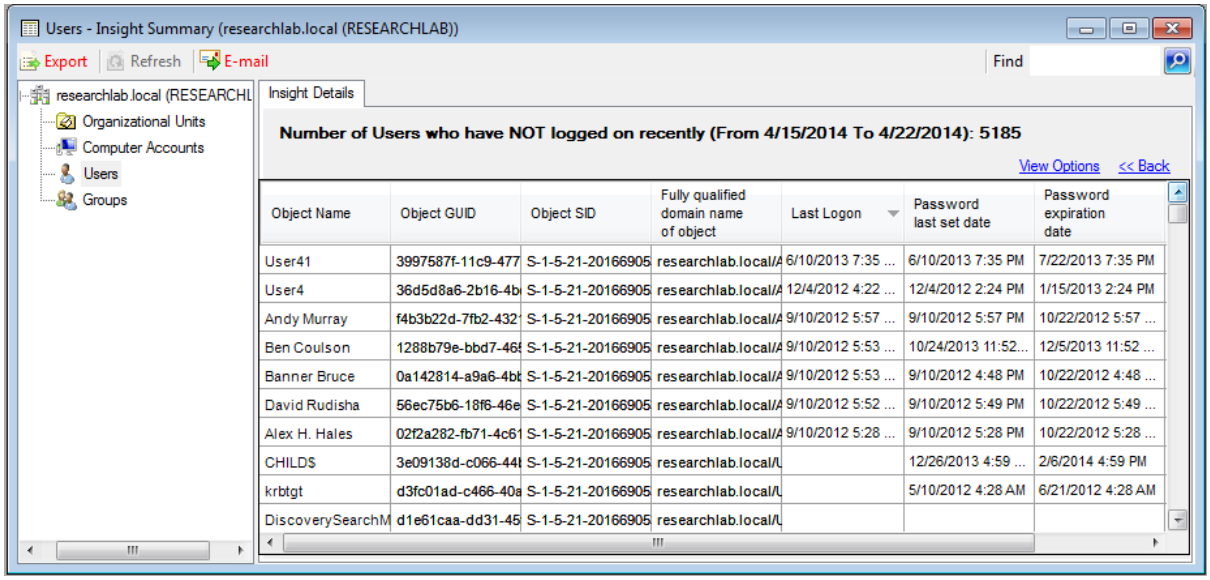
Modify the *parameters* and click **OK** to refresh the report. Note that parameters can be set both in "Summary" and "Details" view of Insight report. Furthermore, parameters can be set on an item-by-item basis only.

NOTE: Some of the reported items may not have parameters to set. If the selected item does not have parameters, then you would see the following message appear on screen:



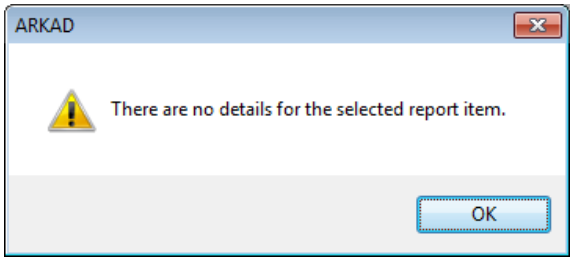
View Details

You can view detailed information of the selected item, by clicking ***View Details*.** Details of the selected item would be displayed as shown below:



To navigate back to the "Summary" view of the Insight report click ***Back.***

NOTE: Some of the reported items may not have any details, for instance, the item that displays the total count of objects. If the selected item does not have details associated with it, then you would see the following message appear on screen:



Items Reported

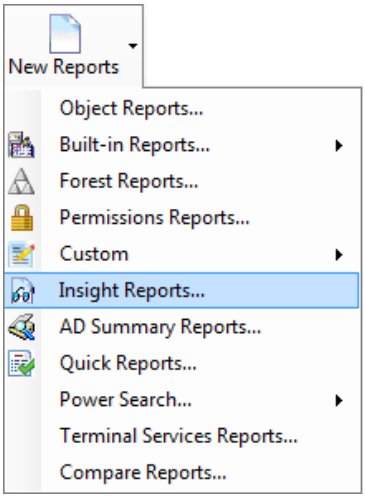
The following table lists the *count-based items* for Users and their corresponding settings:

Count-based Item Name	Description	Parameters	Detail Report
Total number of users	Displays the total count of users in the domain.	None	No detail report
Number of recently created users	Displays the count of user accounts that were created in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Users.
Number of recently modified users	Displays the count of user accounts that were modified in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Users.
Number of recently deleted users	Displays the count of user accounts that were deleted in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Deleted Objects" report for Users.
Number of users required to change their password at next logon	Displays the count of user accounts whose password has expired and are required to change their password at next logon.	None	Displays the "Account" report for Users.
Number of users who cannot change their password	Displays the count of user accounts who cannot change their password.	None	Displays the "Account" report for Users.
Number of users whose password never expires	Displays the count of user accounts whose password never expires.	None	Displays the "Account" report for Users.

Number of User accounts whose password expires in the time period	Displays the count of user accounts whose password expires in the specified time period.	Specify a date-range value (Start and end dates).	Displays the "Additional Account Info" report for Users.
Number of disabled user accounts	Displays the count of user accounts that are disabled.	None	Displays the "Account" report for Users.
Number of locked out user accounts	Displays the count of user accounts that are locked out.	None	Displays the "Account" report for Users.
Number of user accounts that expire	Displays the count of user accounts that are set to expire.	None	Displays the "Account" report for Users.
Number of User accounts that expire in the time period	Displays the count of user accounts that expire in the specified time period.	Specify a date-range value (Start and end dates).	Displays the "Account" report for Users.
Number of users whose password is stored using reversible encryption	Displays the count of users whose password is stored using reversible encryption.	None	Displays the "Account" report for Users.
Number of user accounts that are required to use Smart card for interactive logon	Displays the count of users that are required to use Smart card for logon.	None	Displays the "Account" report for Users.
Number of user accounts that are trusted for delegation	Displays the count of user accounts that are trusted for delegation.	None	Displays the "Account" report for Users.
Number of user accounts that are sensitive and cannot be delegated	Displays the count of user accounts that are sensitive and cannot be delegated.	None	Displays the "Account" report for Users.

Number of user accounts that use DES encryption types for keys	Displays the count of user accounts that use DES encryption types for keys.	None	Displays the "Account" report for Users.
Number of user accounts that do not require Kerberos pre-authentication for logging on	Displays the count of user accounts that do not require Kerberos pre-authentication for logging on.	None	Displays the "Account" report for Users.
Number of users who are member of more than N groups	Displays the count of user accounts that are member of more than the specified number of groups.	Specify number of groups.	Displays the "Member Of" report for Users.
Number of users who have NOT logged on recently	Displays the count of users who have NOT logged on in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "General" report for Users.
Number of users who have logged on recently	Displays the count of users who have logged on in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Additional Account Info" report for Users.
Number of user accounts that expire in the time period	Displays the count of user accounts that expire in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Account" report for Users.

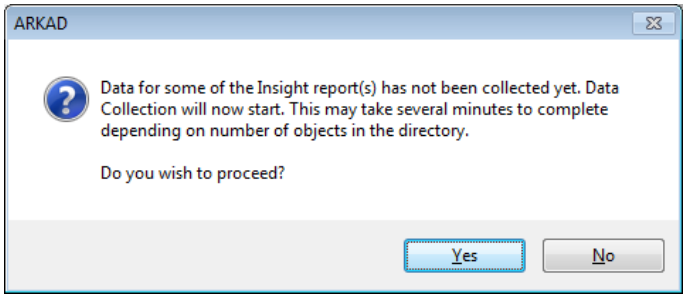
11.5 How to view Insight Report for Groups?



***Click** on* *button.* The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.

Select and expand the domain node in the left pane of the newly launched report window, and then click on **Groups.**

The following message will appear on screen, if the report data has not been already collected:


ARKAD
Data for some of the Insight report(s) has not been collected yet. Data Collection will now start. This may take several minutes to complete depending on number of objects in the directory.
Do you wish to proceed?
Yes
No

Select **yes** to collect data.

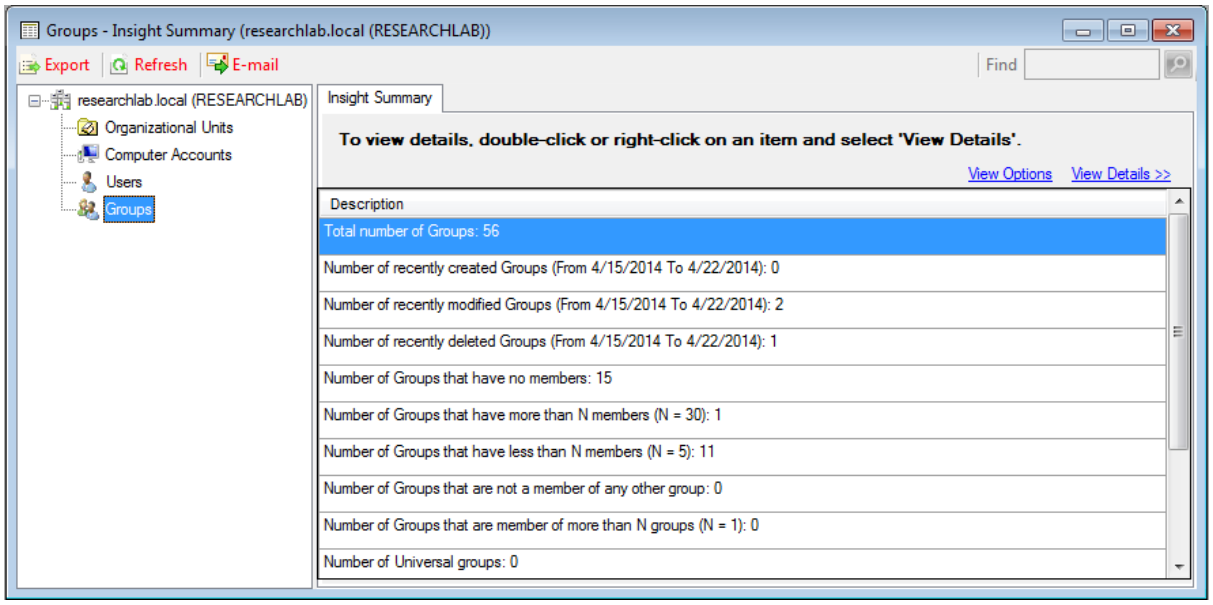
NOTE:

- The Insight report items of an object depend on data from its corresponding "Object Report" tab(s). For instance, the item that displays the count of objects created in a certain time period depends on data from the "Object" tab. So, when the data collection begins, data for all the "Object Report" tab(s) would be collected first, after which the Insight report would be generated.
- If you select **No,** then the required "Object Report(s)" data would not be collected. As a result, you may see zeroes against Insight items for which data is

not available. However, note that, you may select **No** when you refresh Insight report data. In that case the existing report data will remain unchanged.

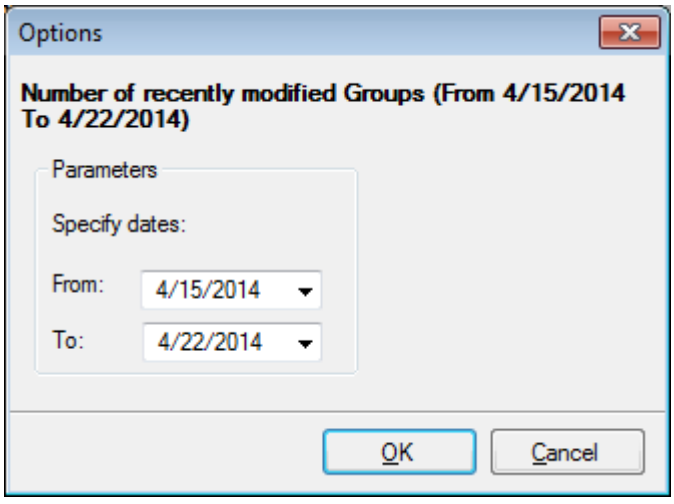
- Also, note that the same message would be displayed when you click ***Refresh Data*** on the tool bar.

The report would be displayed as shown below:


Groups - Insight Summary (researchlab.local (RESEARCHLAB))
Export
Refresh
E-mail
Find
researchlab.local (RESEARCHLAB)
Organizational Units
Computer Accounts
Users
Groups
Insight Summary
To view details, double-click or right-click on an item and select 'View Details'.
View Options
View Details >>
Description
Total number of Groups: 56
Number of recently created Groups (From 4/15/2014 To 4/22/2014): 0
Number of recently modified Groups (From 4/15/2014 To 4/22/2014): 2
Number of recently deleted Groups (From 4/15/2014 To 4/22/2014): 1
Number of Groups that have no members: 15
Number of Groups that have more than N members (N = 30): 1
Number of Groups that have less than N members (N = 5): 11
Number of Groups that are not a member of any other group: 0
Number of Groups that are member of more than N groups (N = 1): 0
Number of Universal groups: 0

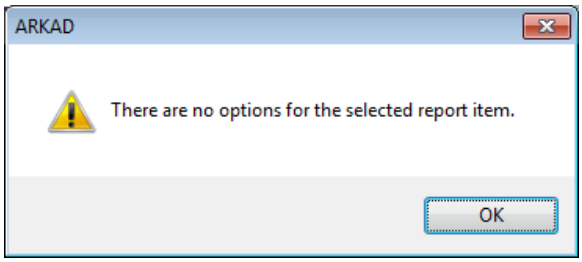
View Options

You can modify parameters of the selected item by clicking on ***View Options*** and get the desired report. The ***Options*** dialog would be displayed as shown below:



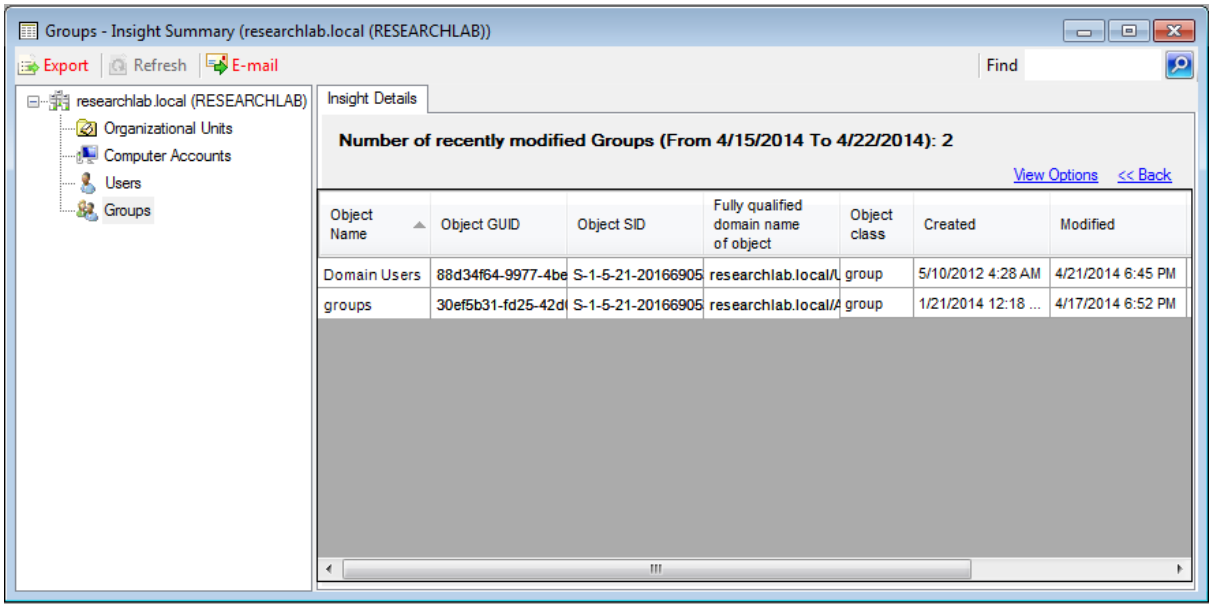
Modify the ***parameters*** and click ***OK*** to refresh the report. Note that parameters can be set both in "Summary" and "Details" view of Insight report. Furthermore, parameters can be set on an item-by-item basis only.

NOTE: Some of the reported items may not have parameters to set. If the selected item does not have *parameters*, then you would see the following message appear on screen:



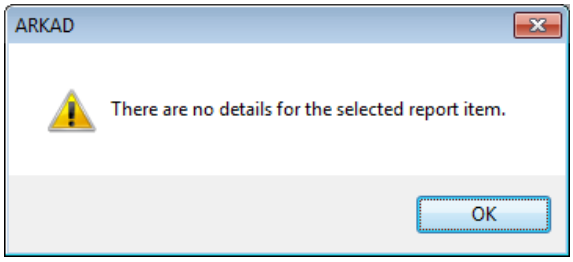
View Details

You can view detailed information of the selected item by clicking ***View Details*.** Details of the selected item would be displayed as shown below:



To navigate back to the "Summary" view of the Insight report click *Back.*

NOTE: Some of the reported items may not have any details, for instance, the item that displays the total count of objects. If the selected item does not have details associated with it, then you would see the following message appear on screen:



Items Reported

The following table lists the *count-based items* for Groups and their corresponding settings:

Count-based Item Name	**Description**	**Parameters**	**Detail Report**
Total number of groups	Displays the total count of Groups in the domain.	None	No detail report
Number of recently created groups	Displays the count of groups that were created in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Groups.
Number of recently modified groups	Displays the count of groups that were modified in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Object" report for Groups.
Number of recently deleted groups	Displays the count of groups that were deleted in a specified time period.	Specify a date-range value (Start and end dates).	Displays the "Deleted Objects" report for Groups.
Number of groups that have no members	Displays the count of groups that are empty.	None	Displays the "Object" report for Groups.
Number of groups that have more than N members	Displays the count of groups that have more than the specified number of members.	Specify number of members.	Displays "Members" report for Groups.
Number of groups that have less than N members	Displays the count of groups that have number of members less than the specified number.	Specify number of members.	Displays "Members" report for Groups.
Number of groups that are not a member of any other group	Displays the count of groups that are not a member in any group.	None	Displays "General" report for Groups.

Number of groups that are member of more than N groups	Displays the count of groups that are a member in more than the specified number of groups.	Specify number of groups	Displays "Member Of" report for Groups.
Number of universal groups	Displays the count of universal groups.	None	Displays "General" report for Groups.
Number of global groups	Displays the count of global groups.	None	Displays "General" report for Groups.
Number of domain local groups	Displays the count of domain local groups.	None	Displays "General" report for Groups.
Number of distribution groups	Displays the count of distribution groups.	None	Displays "General" report for Groups.
Number of security groups	Displays the count of security groups.	None	Displays "General" report for Groups.

Chapter 13

12 Power Search

12.1 About Power Search

The ***Power Search*** feature allows the user to *perform search* for specific permission(s) assigned in objects available in Active Directory domain. Based on the nature of usage in Active Directory, the *permissions* in this feature have been classified as stated below:

Permission Type	Permission Description
General	Basic set of permissions that is normally seen, when security tab is opened.
Special	Special set of permissions with a broad control over objects. These permissions can be viewed in Advanced Security Settings for an AD Object.
Special (Advanced)	Detailed permissions that provides granular access/restrictions on objects. This permission can be viewed in Advanced Security Settings for an AD object. The sub-categories that fall under this category are **1)** Property-Specific permissions - Related to Active Directory object's properties. **2)** Creation/Deletion-Specific permissions - Related to Active Directory objects.
Extended-Rights	Extended rights are the additional rights that do not involve read/write access to individual object attributes. It refers to the permission for certain administrative actions on object attributes, such as changing a user's password.
Common Tasks	This forms the list of permission tasks (similar to delegation) where in each task is equivalent to a set of permissions. Permissions through delegation may be searched under this classification of permissions.

CHAPTER-12-Power Search

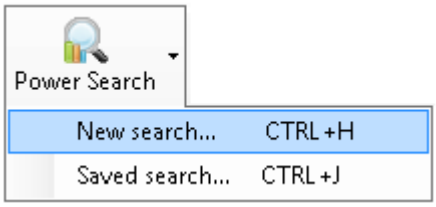
Currently, the Power Search feature supports User, Group, Contact, Computer, Organizational Unit and Domain Controller objects in Active Directory.

The benefits of Power Search are as follows:

- *Permissions* are *classified* on well-known standards for easy understanding by AD administrators.
- *Permissions are retrieved directly from domain controller's schema definition and shown for selection. Hence, any change to the AD schema will get reflected in reported permissions.*
- Ability to ***save*** *the* ***search*** for repeated use.
- Can ***export and email*** the generated reports.

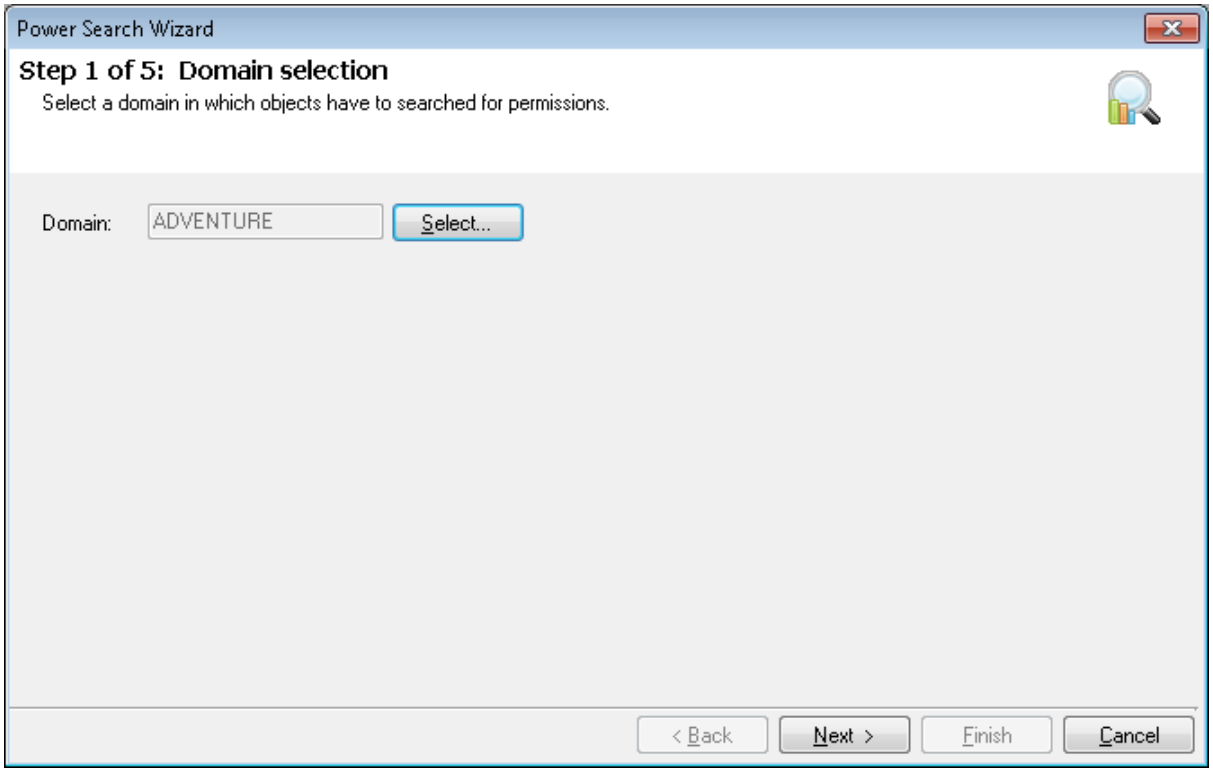
12.2 How to Perform a New Power Search?

The ***New Search*** option in ***Power Search*** feature allows you to generate a security permissions search report through Power Search Wizard. The Power Search Wizard will guide you through the following step to perform a new security permission search. You can either save the search report or leave it unsaved.

To launch ***Power Search*** Wizard, *click* 

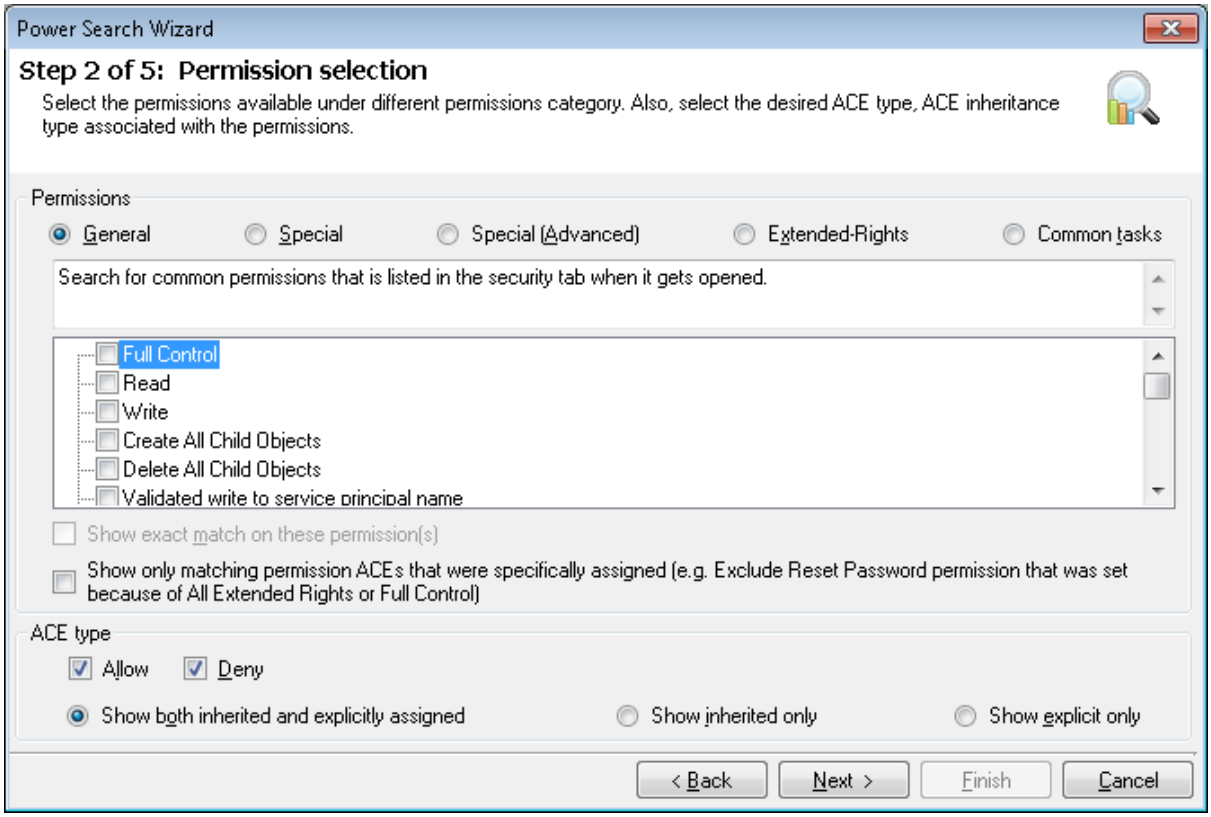
menu in the toolbar. The ***Power Search Wizard*** will appear as shown below:

Step 1: Domain Selection



- *Select* a *domain* by *clicking* ***Select...*** button. Upon clicking this button, the Connection Manager will be displayed from which you can select a *domain.*
- *Click Next* to Proceed to the ***Next*** Step.

Step 2: Permission Selection


Power Search Wizard
Step 2 of 5: Permission selection
Select the permissions available under different permissions category. Also, select the desired ACE type, ACE inheritance type associated with the permissions.
Permissions
General
Special
Special (Advanced)
Extended-Rights
Common tasks
Search for common permissions that is listed in the security tab when it gets opened.
Full Control
Read
Write
Create All Child Objects
Delete All Child Objects
Validated write to service principal name
Show exact match on these permission(s)
Show only matching permission ACEs that were specifically assigned (e.g. Exclude Reset Password permission that was set because of All Extended Rights or Full Control)
ACE type
Allow
Deny
Show both inherited and explicitly assigned
Show inherited only
Show explicit only
< Back
Next >
Finish
Cancel

- *Select* the desired *permissions category***,** and the permissions to be searched under ***Permissions*** *section:*
- *Select* the ***'Show exact match on these permission(s)'*** *checkbox,* if you wish to view only the exact match of the selected permissions and not the sub-set of permissions.
- *Select* 'Show only matching permission ACEs that were specifically assigned (e.g. Exclude Reset Password permission that was set because of All Extended Rights or Full Control)' checkbox to limit the search to check for only specifically assigned permissions.
- *Select* the desired ***Access Control Entry*** type under ***'ACE type'*** section.
- *Select* the desired ***permission inheritance*** type under ***'ACE type'*** section.

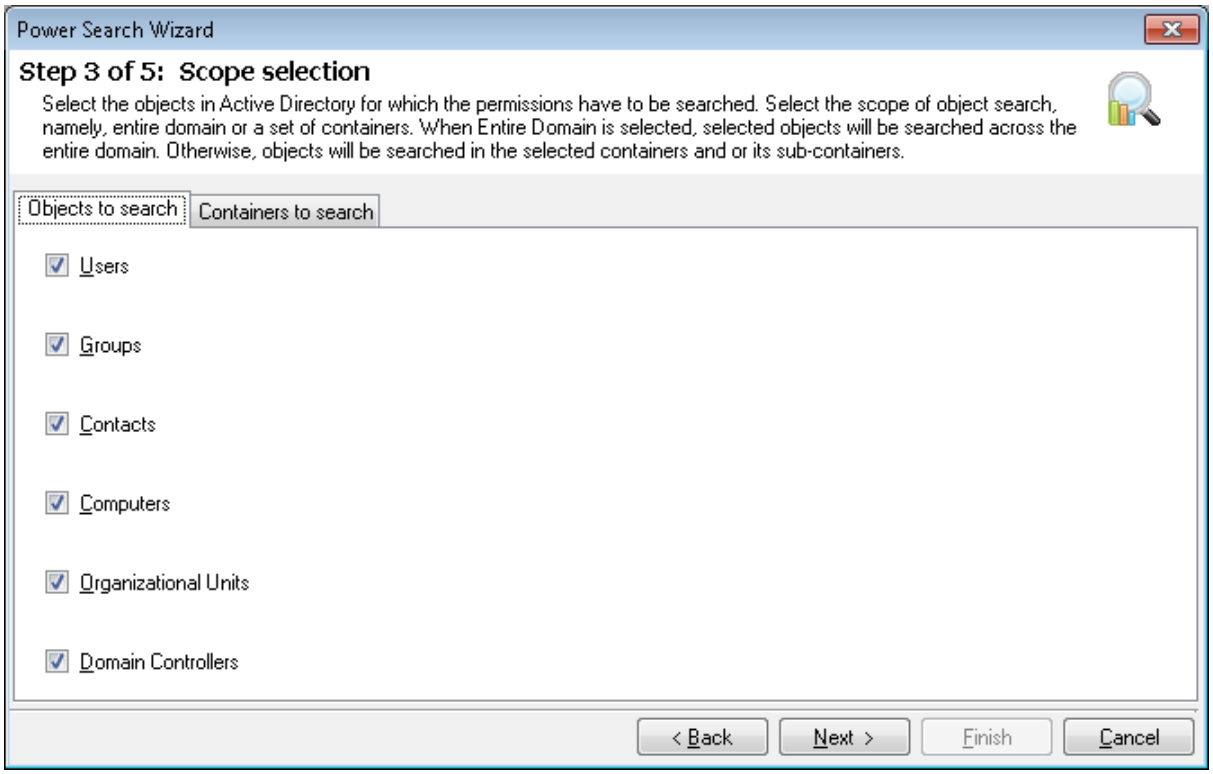
  Show both inherited and explicitly assigned - to view both *inherited* and *explicitly assigned* permissions.

  Show inherited only - to view only *inherited permissions.*

  Show explicit only - to view only *explicitly assigned permissions.*
- *Click Next* to Proceed to the ***Next*** Step.

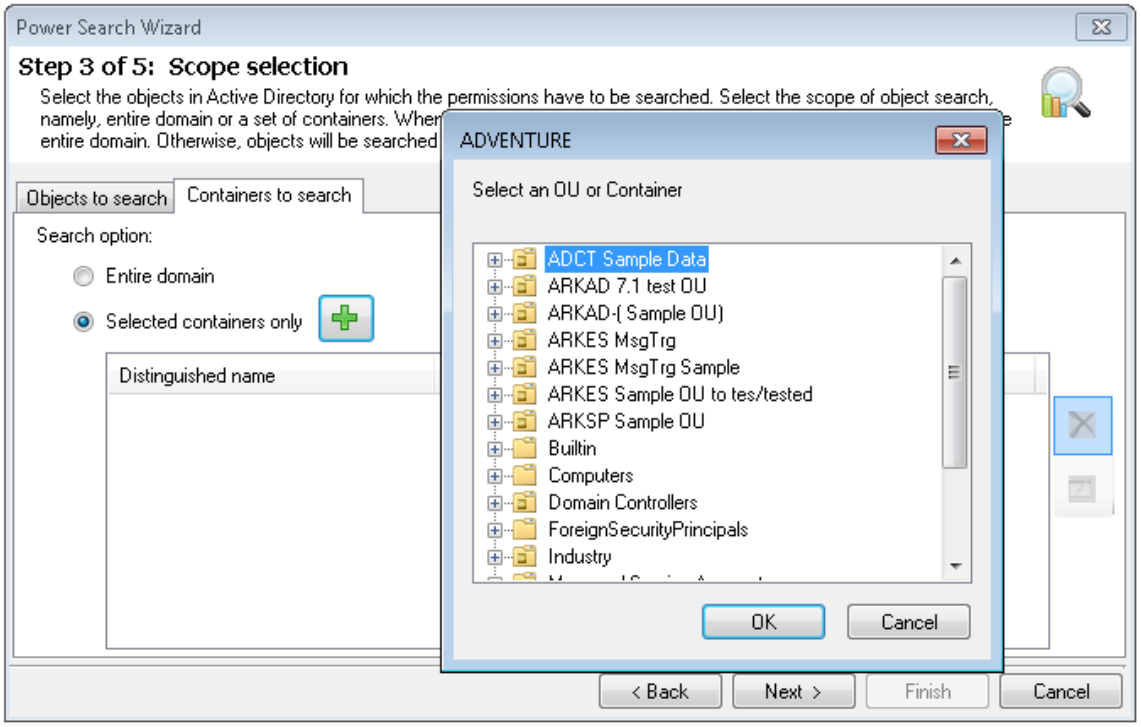
Step 3: Scope Selection

- *Select* the type of objects under ***'Objects to search'*** tab for which the selected permissions have to be searched. The ***objects*** corresponding to the selected ***object types*** will be enumerated in the connected domain and permissions will be searched for them.

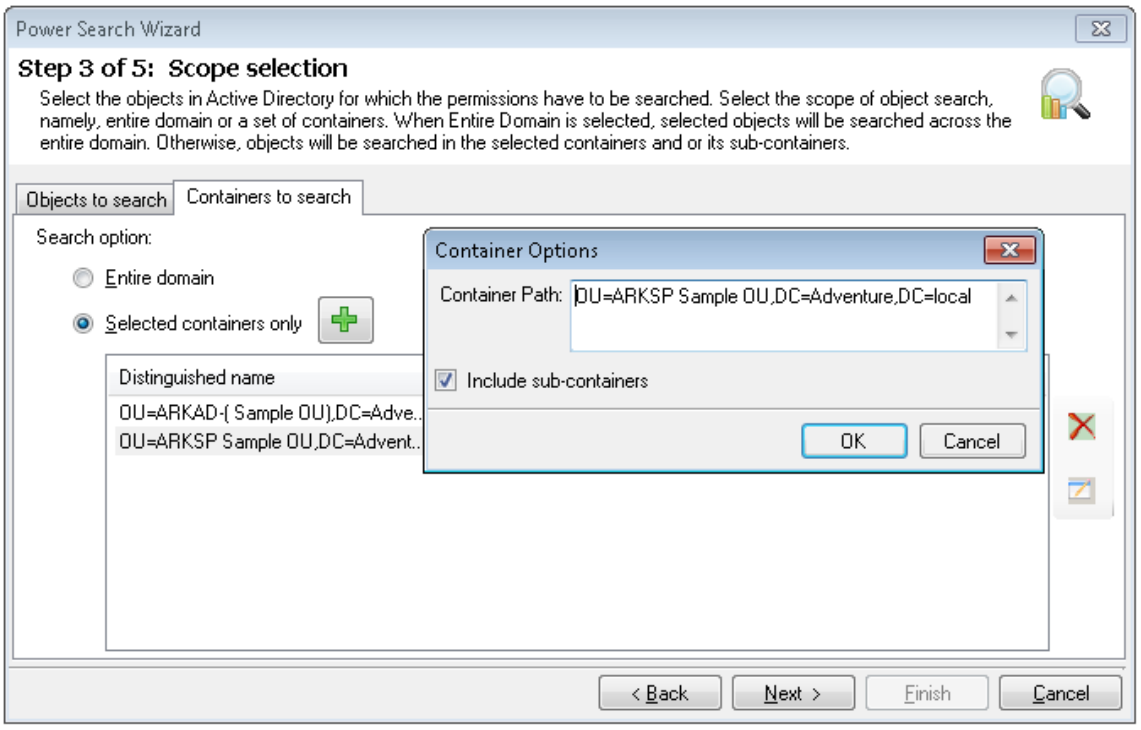

Power Search Wizard
Step 3 of 5: Scope selection
Select the objects in Active Directory for which the permissions have to be searched. Select the scope of object search, namely, entire domain or a set of containers. When Entire Domain is selected, selected objects will be searched across the entire domain. Otherwise, objects will be searched in the selected containers and or its sub-containers.
Objects to search
Containers to search
Users
Groups
Contacts
Computers
Organizational Units
Domain Controllers
< Back
Next >
Finish
Cancel

NOTE: If the permissions category selected in the previous step is Common tasks, then the ***'Objects to search'*** tab is not applicable.

- Under ***'Containers to search'*** tab, *select* the suitable *option (Entire domain or a sub-set of containers)* in which selected type of objects have to be enumerated. You can select a set of containers in the domain by using ***'+' button*** to restrict the search scope of objects.



- By default, ARKAD processes the sub-containers of the selected containers to enumerate objects. You can click **'Edit Options'** button to change this behavior.

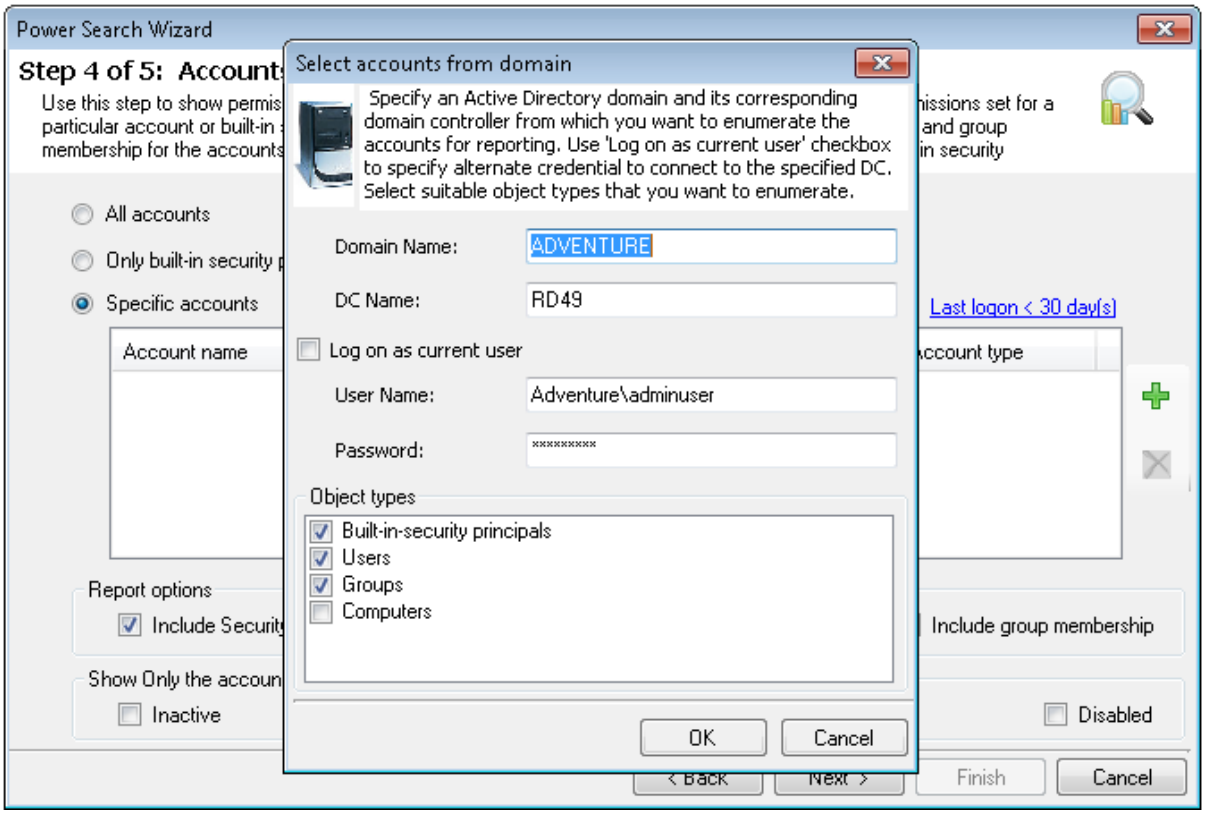

Power Search Wizard
Step 3 of 5: Scope selection
Select the objects in Active Directory for which the permissions have to be searched. Select the scope of object search, namely, entire domain or a set of containers. When Entire Domain is selected, selected objects will be searched across the entire domain. Otherwise, objects will be searched in the selected containers and or its sub-containers.
Objects to search
Containers to search
Search option:
Entire domain
Selected containers only
Distinguished name
OU=ARKAD-(Sample OU),DC=Adve..
OU=ARKSP Sample OU,DC=Advent..
Container Options
Container Path:
OU=ARKSP Sample OU,DC=Adventure,DC=local
Include sub-containers
OK
Cancel
< Back
Next >
Finish
Cancel

- *Click* **Next** to Proceed to the Next Step.

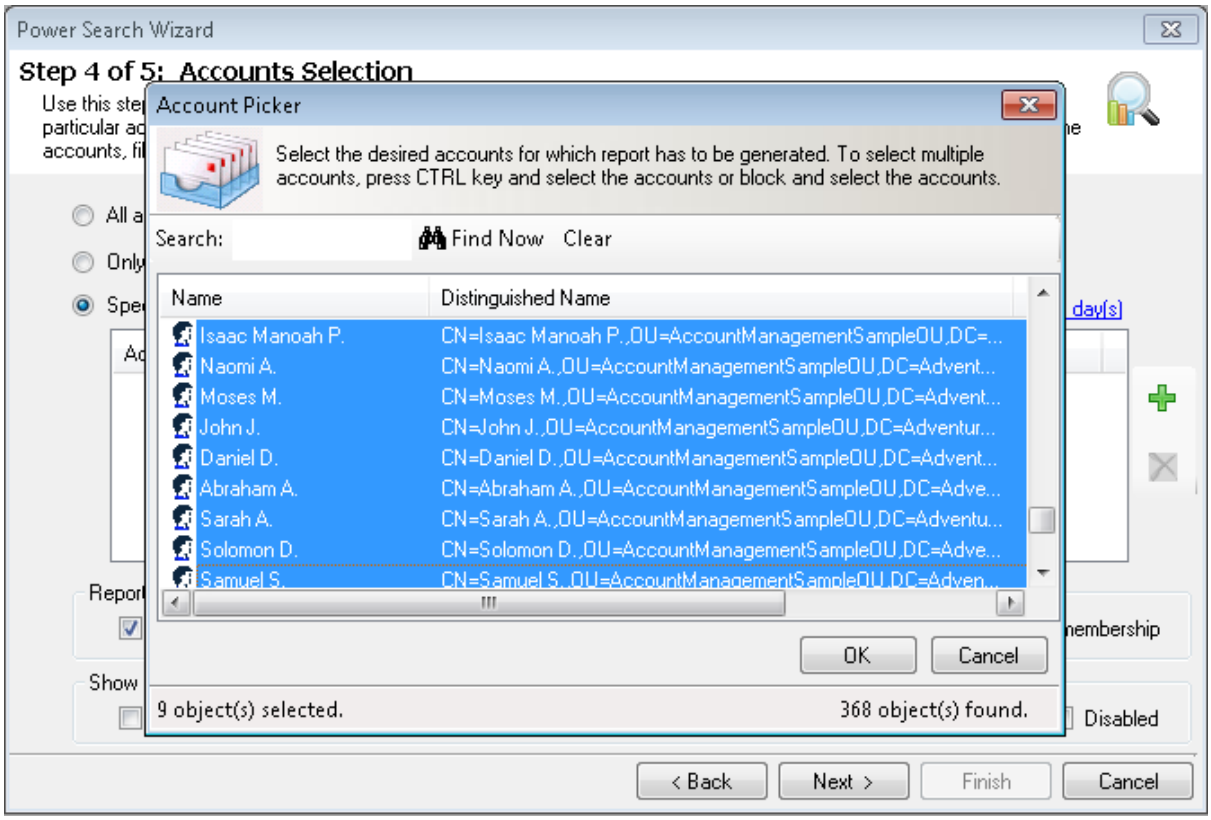
Step 4: Accounts Selection

Power Search Wizard
Step 4 of 5: Accounts Selection
Use this step to show permissions for a selected set of accounts. For example, you may search for a permissions set for a particular account or built-in security principals. You can enhance the report information by including SID and group membership for the accounts, filtering inactive, unknown, expired and disabled accounts, excluding built-in security
All accounts
Only built-in security principals
Specific accounts
Inactive account threshold : Last logon < 30 day(s)
Account name
Distinguished name
Account type
Report options
Include Security Identifier (SID)
Exclude built-in security principals
Include group membership
Show Only the accounts
Inactive
Unknown
Expired
Disabled
< Back
Next >
Finish
Cancel

- Select the list of accounts for which the selected permissions on objects have to be reported. In this section, select the suitable option ***(All accounts or a set of accounts)*** for which permissions will be reported.
- You can select 'Only built-in security principals' option to list only the built-in security principals (assigned in security settings) in the permission reports.
- You can select a set of accounts ***(Built-in-security principals, User, Group, Computers)*** from different domains by using **'+' button.** You can enter ***domain name, domain controller name, user credential*** to connect and enumerate the selected object types.



- The enumerated accounts will be listed in ***'Account Picker'*** dialog as shown below:



You can enter a part of the name to ***search*** and click ***Find Now*** to get the *results*. ***Select*** the desired ***accounts*** and click ***OK***.

- You can also use additional options such as 'Report options' and 'Show only the accounts' as stated below:

Report options - This option can be used to include security identifier (SID), group membership (Member of) of the accounts and to exclude built-in security principals in the report.

Show only the accounts - This option can be used to filter account based on its status. You can filter the accounts that are inactive, unknown, expired and disabled.

Inactive: By default, an account whose 'Last logon' is less than 30 days is considered as inactive accounts. This threshold can be customized, by clicking the hyperlink next to 'Inactive account threshold'.

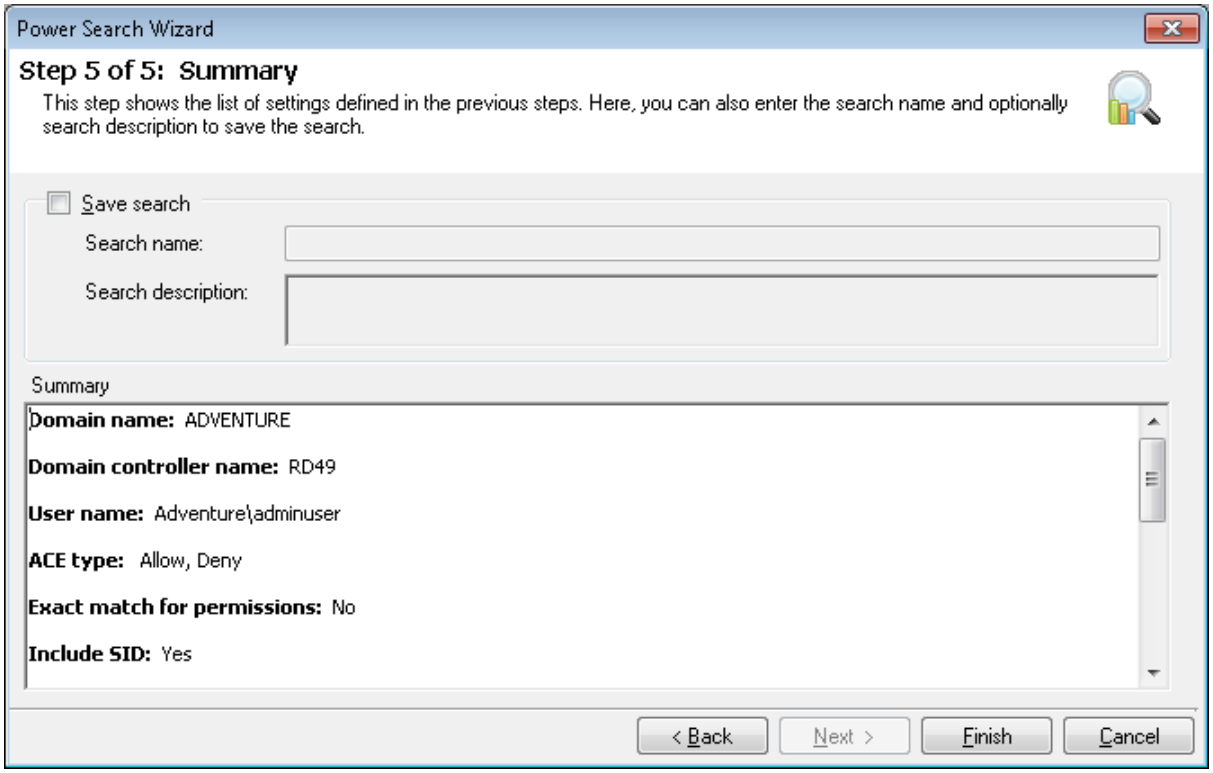
Unknown: The accounts that cannot be identified in a domain. For example, account name like 'Account Unknown S-1-2 ...' can be seen in any objects 'Security' tab, because the corresponding account is deleted and unknown to domain. The unknown account will also include Foreign Security Principals.

Expired: The accounts that are already expired.

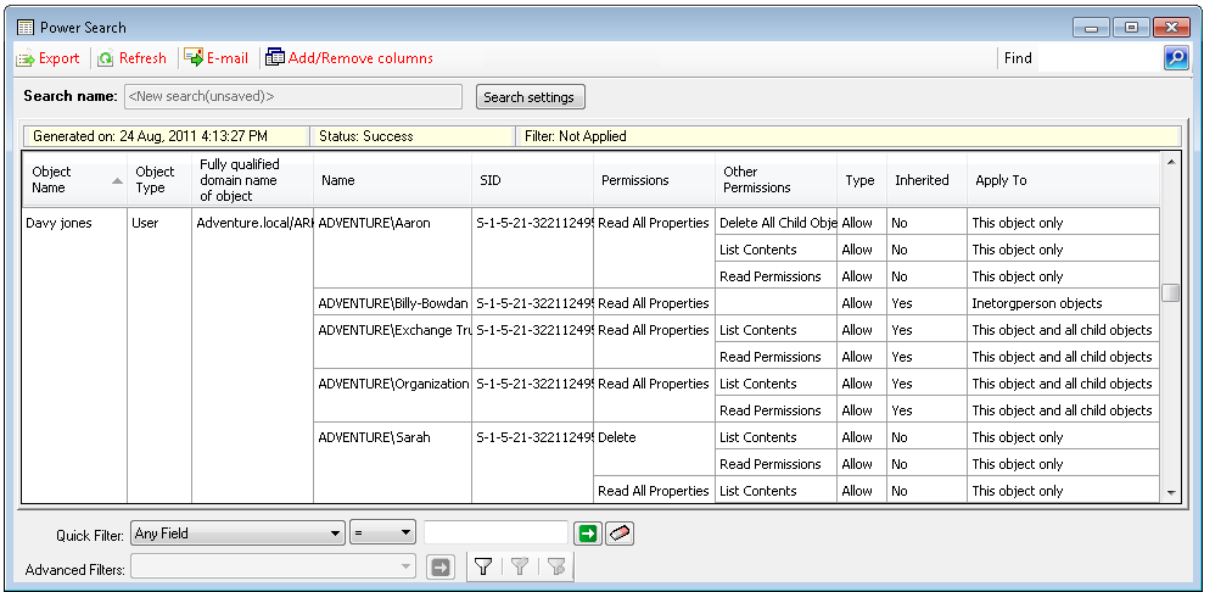
Disabled: The accounts that are disabled.

- Click ***Next*** to Proceed to the next step.

Step 5: Summary


Power Search Wizard
Step 5 of 5: Summary
This step shows the list of settings defined in the previous steps. Here, you can also enter the search name and optionally search description to save the search.
Save search
Search name:
Search description:
Summary
Domain name: ADVENTURE
Domain controller name: RD49
User name: Adventure\adminuser
ACE type: Allow, Deny
Exact match for permissions: No
Include SID: Yes
< Back
Next >
Finish
Cancel

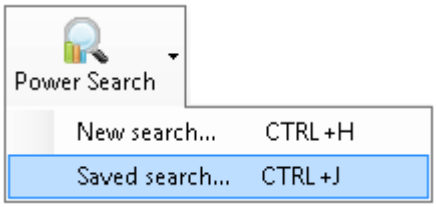
- This step shows the list of settings configured in the previous steps. Verify the settings and click Back to change the settings, if necessary.
- *Select **'Save search'** check box* and enter a ***search name*** and ***search description*** (optional) to save the Power Search for repeated use in the future.
- *Click **Finish** to* generate the report.
- After the data collection process is complete, the report would be generated in a report window as shown below:



- In the report window, you can click the ***'Search settings'*** button to view the search settings associated with the report.

12.3 How to Manage Power Search Reports?

Power Search Manager

Click 

or press CTRL+J to open the **Power Search Manager** window.

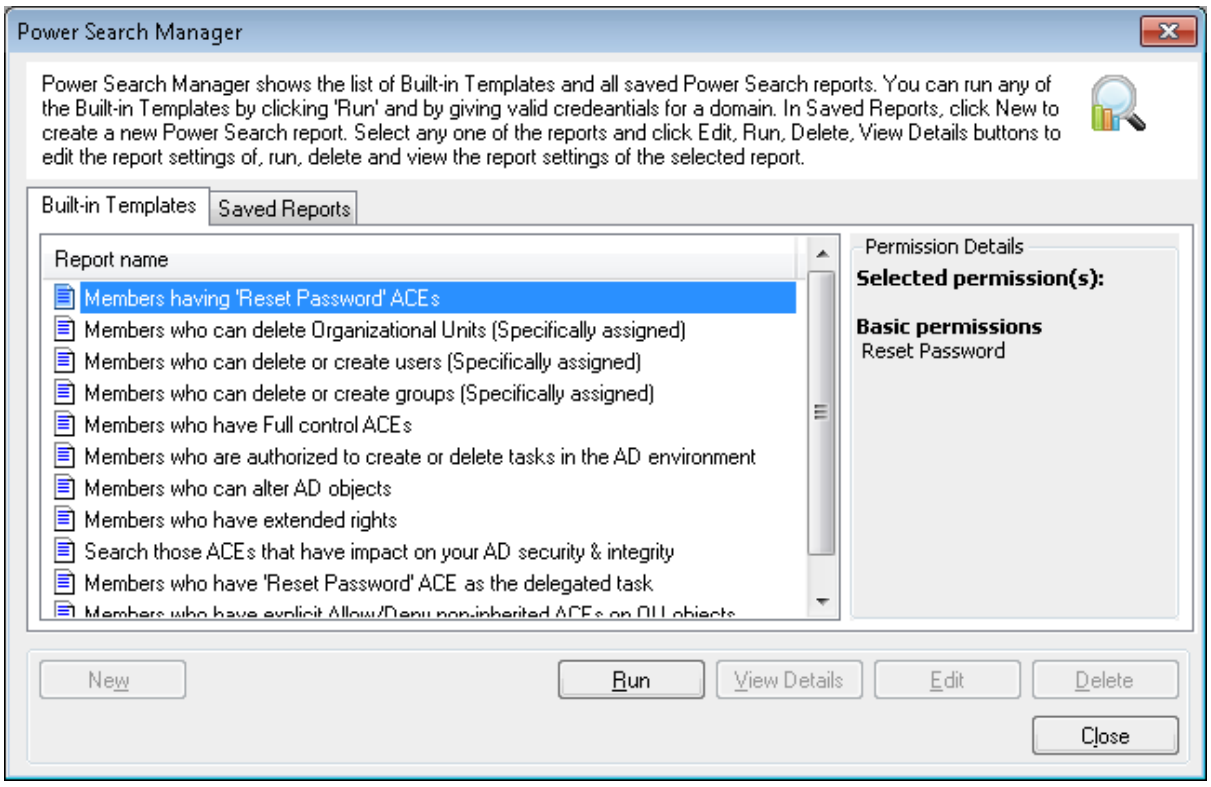
Power Search Manager is broadly classified into two sections namely:

1) Built-in Templates
2) Saved Reports

Built-in Templates:

Built-in Templates comprises of most commonly searched permissions in Active Directory. It cannot be edited or deleted. Also you cannot create a new template, as the templates are generated by **ARKAD** itself.

Run a Built-in template:


Power Search Manager
Power Search Manager shows the list of Built-in Templates and all saved Power Search reports. You can run any of the Built-in Templates by clicking 'Run' and by giving valid credeantials for a domain. In Saved Reports, click New to create a new Power Search report. Select any one of the reports and click Edit, Run, Delete, View Details buttons to edit the report settings of, run, delete and view the report settings of the selected report.
Built-in Templates
Saved Reports
Report name
Members having 'Reset Password' ACEs
Members who can delete Organizational Units (Specifically assigned)
Members who can delete or create users (Specifically assigned)
Members who can delete or create groups (Specifically assigned)
Members who have Full control ACEs
Members who are authorized to create or delete tasks in the AD environment
Members who can alter AD objects
Members who have extended rights
Search those ACEs that have impact on your AD security & integrity
Members who have 'Reset Password' ACE as the delegated task
Permission Details
Selected permission(s):
Basic permissions
Reset Password
New
Run
View Details
Edit
Delete
Close

To run a Built-in template, select the template to be run from Built-in Templates section and click 'Run' button. The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The report window will be launched after the domain and the selected domain controller are validated.

Saved Reports:

Saved Reports are the reports which can be created by the user. Using Saved Reports you can perform the following operations:

Create a new Power Search report

1) Edit a Power Search report
2) View settings configured for Power Search report
3) Delete a Power Search report
4) Run a Power Search report immediately

Create a new Power Search report

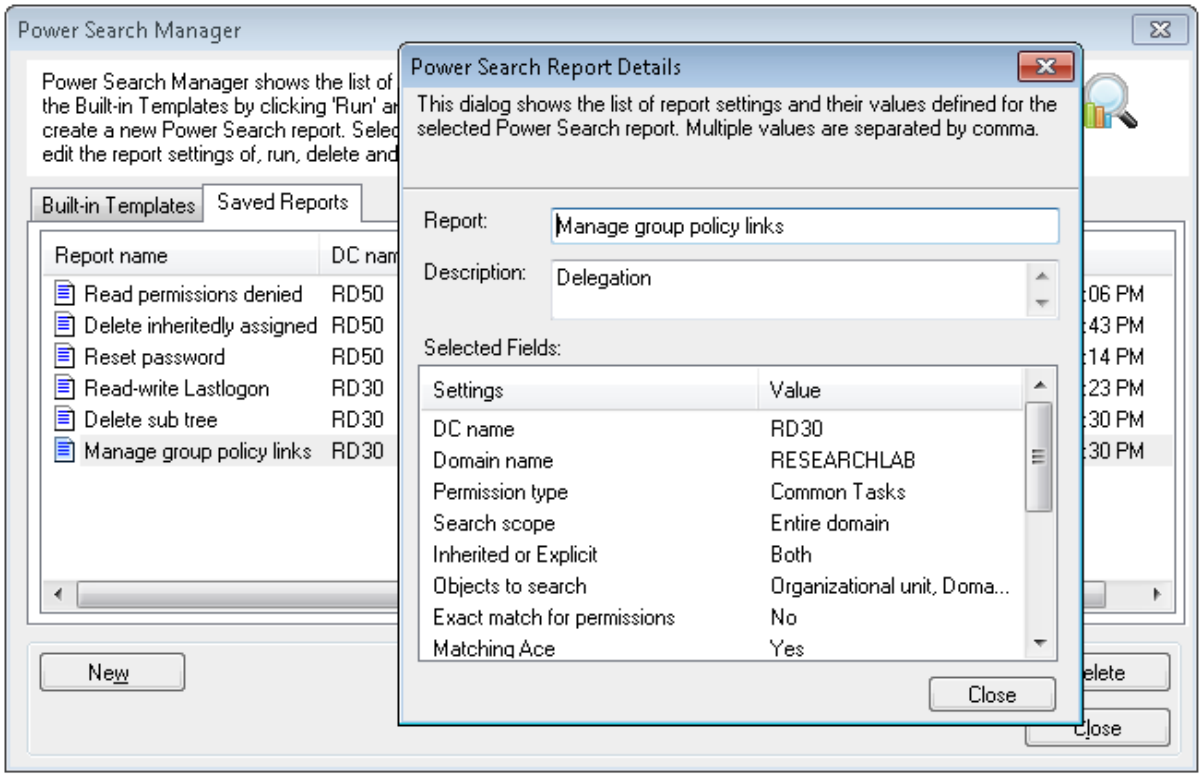
- To create a new Power Search report, click 'New' button in the 'Power Search Manager' window's **Saved Reports** section. The Power Search Wizard will appear on the screen.
- Follow the steps 1 through 3 as outlined in how to perform a new Power Search?
- In step 4, enter a suitable search name to save the new search.

Edit a Power Search report

To edit a Power Search report, click 'Edit' button in the Power Search Manager window's Saved Reports section. The Power Search Wizard will appear on the screen which will guide you through the edit operation. During edit operation, you can modify the list of settings for a report except for the report description. Refer Additional note.

View Settings Configured for Power Search Report

To view the details of a saved Power Search report, select a report and click 'View Details' button in the Power Search Manager window's Saved Reports section. The saved report name, description and the list of settings and their values defined for the selected Power Search report will be displayed in Power Search Details window.



Delete a Power Search Report

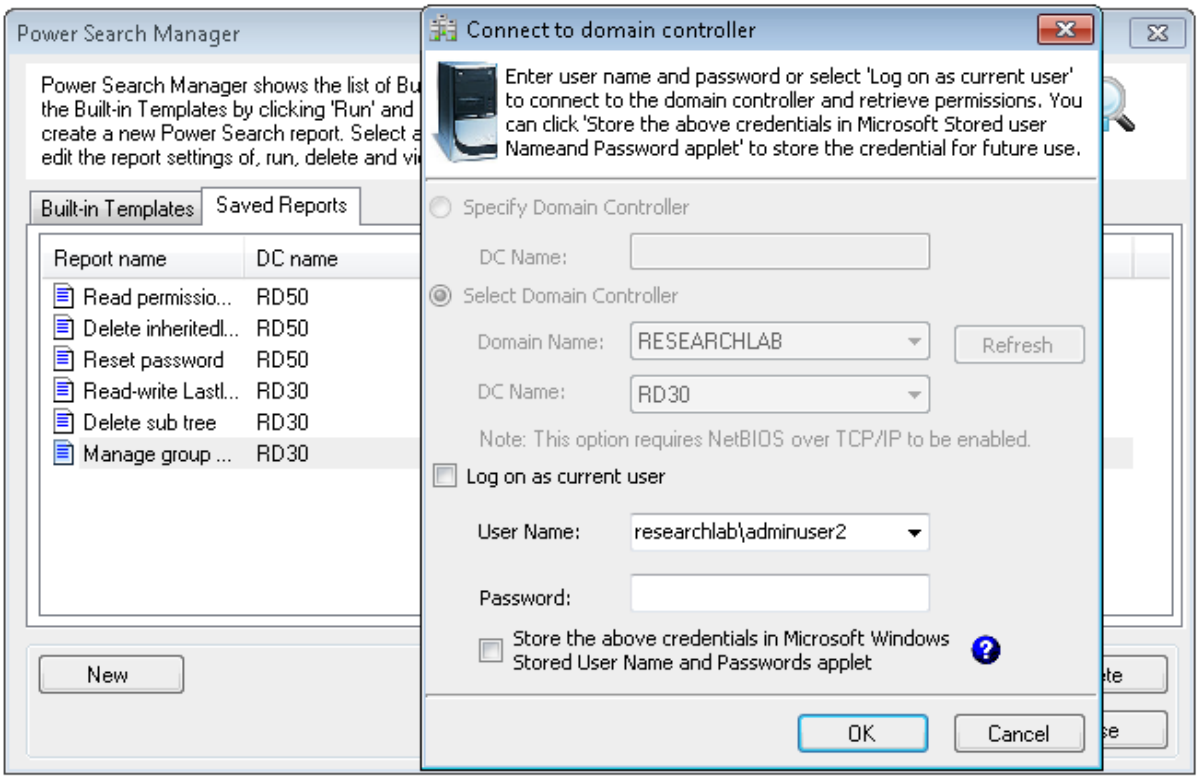
To delete a Power Search report, select the report to be deleted and click 'Delete' button in the Power Search Manager window's Saved Reports section.

Run a Power Search Report immediately

To run a Power Search report, select the report to be run and click 'Run' button in the Power Search Manager window's Saved Reports section.

Additional Note:

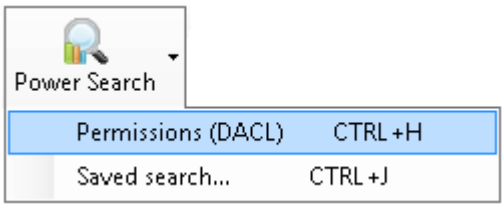
Power Search Wizard will show the ***'Connect to domain controller'*** dialog when it is unable to connect using the ***credential*** specified during the creation of Power Search report that is being edited/run.


Power Search Manager
Power Search Manager shows the list of Bu
the Built-in Templates by clicking 'Run' and
create a new Power Search report. Select a
edit the report settings of, run, delete and vi
Built-in Templates
Saved Reports
Report name
DC name
Read permissio...
RD50
Delete inheritedl...
RD50
Reset password
RD50
Read-write Lastl...
RD30
Delete sub tree
RD30
Manage group ...
RD30
New
Connect to domain controller
Enter user name and password or select 'Log on as current user' to connect to the domain controller and retrieve permissions. You can click 'Store the above credentials in Microsoft Stored user Nameand Password applet' to store the credential for future use.
Specify Domain Controller
DC Name:
Select Domain Controller
Domain Name:
RESEARCHLAB
Refresh
DC Name:
RD30
Note: This option requires NetBIOS over TCP/IP to be enabled.
Log on as current user
User Name:
researchlab\adminuser2
Password:
Store the above credentials in Microsoft Windows Stored User Name and Passwords applet
OK
Cancel

If the credential is not set to store in ARKAD's Profile Manager, the application will prompt for *password* while you try to edit or run a Power Search report. You can ***save the credentials*** in Profile manager by checking the ***'Store the above user credentials in Microsoft Windows Stored User Name and Passwords applet'*** check box in the Connection Manager.

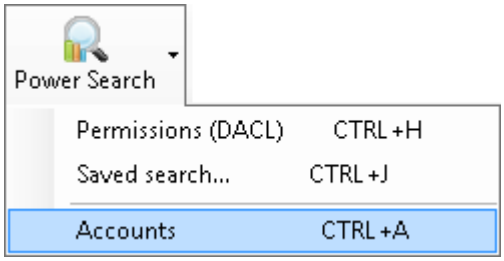
12.4 How to Generate Power Search Reports?

You can ***generate*** a ***Power Search report*** by using any of the following options:

- ***Selecting*** 

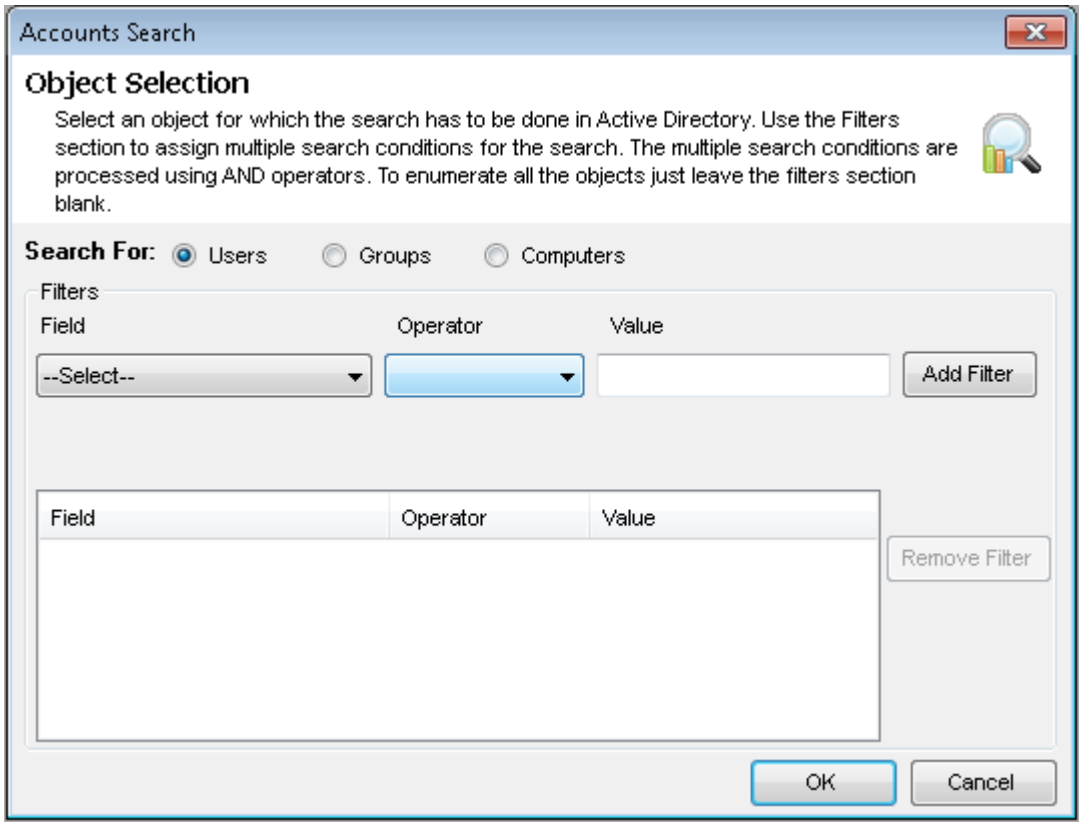
menu in the toolbar (Also refer "How to perform a new Power Search?").
- Clicking ***'Run'*** button in the ***Power Search Manager*** window (Also refer "Run a Power Search report immediately").

12.5 How to Perform a New Account Search?

Select 

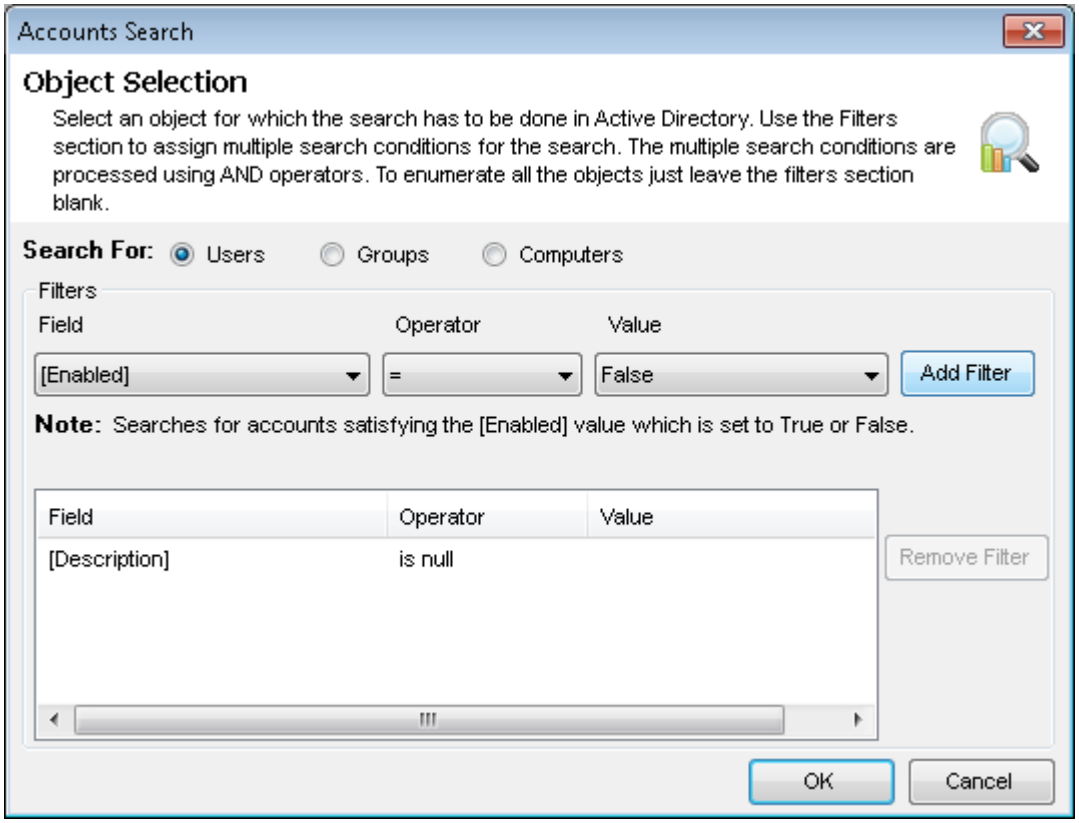
menu in the toolbar. The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller.

The **Accounts Search** dialog will be launched after the domain and the selected domain controller are validated as shown below:


Accounts Search
Object Selection
Select an object for which the search has to be done in Active Directory. Use the Filters section to assign multiple search conditions for the search. The multiple search conditions are processed using AND operators. To enumerate all the objects just leave the filters section blank.
Search For: Users Groups Computers
Filters
Field
Operator
Value
--Select--
Add Filter
Field
Operator
Value
Remove Filter
OK
Cancel

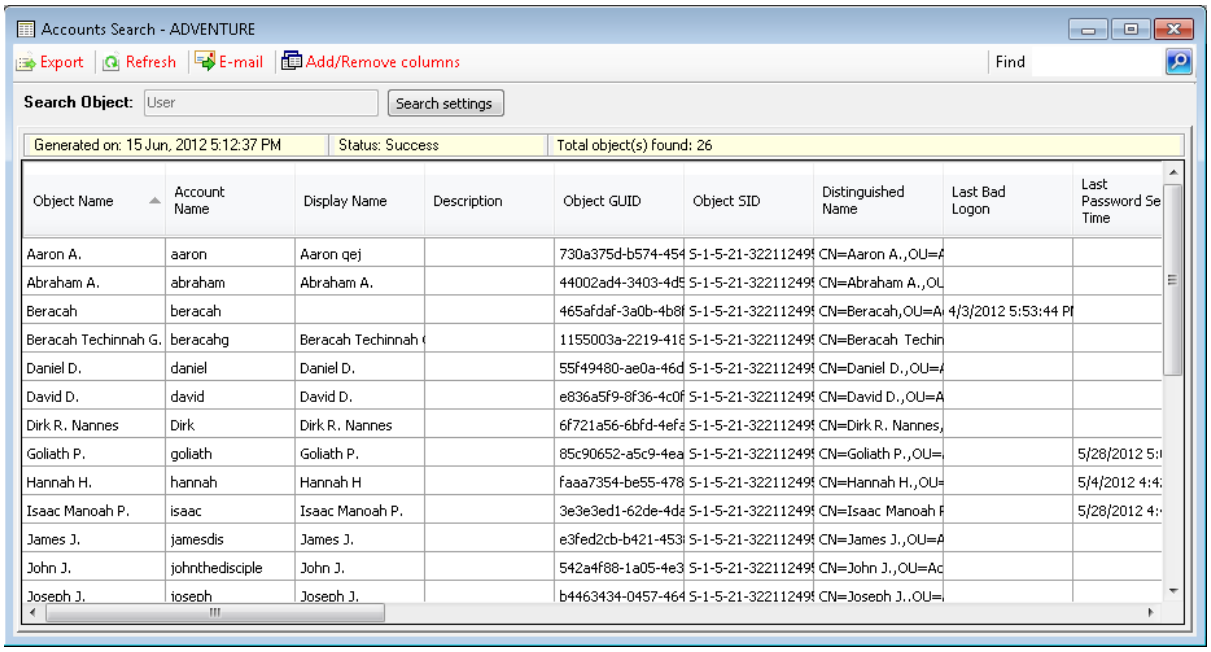
In the **Accounts Search** dialog,

- *Select* an object **(Computers or Users or Groups)** for which the search has to be done in Active Directory.
- Use the **Filters** section to assign multiple search conditions for the search by selecting a **Field,** an **Operator** and specify a **Value** for the condition. The multiple search conditions are processed using **AND** operators.
- *Click* **Add Filter** to *add* the *filter* to the *list* as shown below:

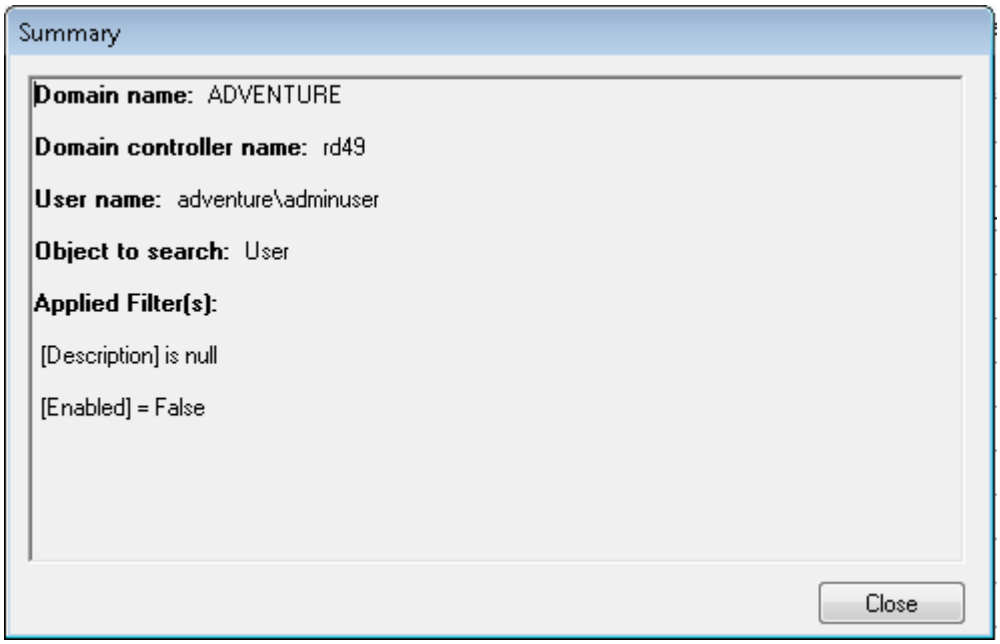

Accounts Search
Object Selection
Select an object for which the search has to be done in Active Directory. Use the Filters section to assign multiple search conditions for the search. The multiple search conditions are processed using AND operators. To enumerate all the objects just leave the filters section blank.
Search For: Users Groups Computers
Filters
Field
Operator
Value
[Enabled]
=
False
Add Filter
Note: Searches for accounts satisfying the [Enabled] value which is set to True or False.
Field
Operator
Value
[Description]
is null
Remove Filter
OK
Cancel

- After *adding* the desired *filters click* **OK** to perform the search.
- To enumerate all the objects just leave the *filters* section *blank and click* **OK.**

After the data collection process is complete, the report would be generated in a report window as shown below:



In the report window, *click* **Search settings** to view the *search settings* associated with the report as shown below:



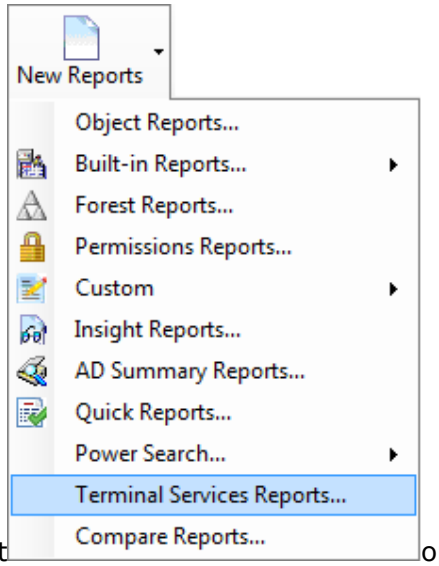
Chapter 13

13 How to generate Terminal Services Reports?

13.1 About Terminal Services Reports

The Terminal Services Reports feature in ARKAD is used to retrieve Terminal Services or Remote Desktop Services information of roaming users in a domain. Valuable information like Terminal services profile path (Roaming User Profile path), Terminal services home directory, allow logon,... etc can be retrieved using this feature.

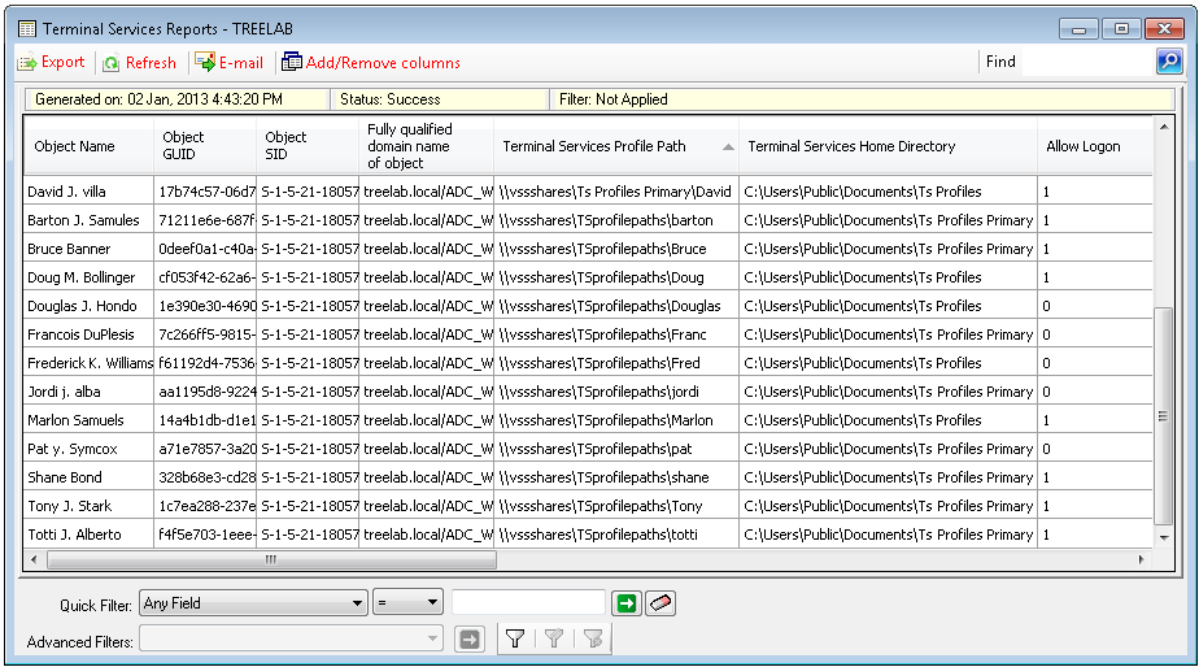
13.2 How to generate Terminal Services Reports?



Select option under New Reports button. The Connection Manager will appear on the screen which will allow you to select a domain and a corresponding domain controller. The data collection process will start after the domain and the selected domain controller are validated.

CHAPTER-12-Power Search

After the data collection process is complete, the report would be generated in a report window as shown below:



Object Name	Object GUID	Object SID	Fully qualified domain name of object	Terminal Services Profile Path	Terminal Services Home Directory	Allow Logon
David J. villa	17b74c57-06d7	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\Ts Profiles Primary\David	C:\Users\Public\Documents\Ts Profiles	1
Barton J. Samules	71211e6e-687f	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\barton	C:\Users\Public\Documents\Ts Profiles Primary	1
Bruce Banner	0deef0a1-c40a	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\Bruce	C:\Users\Public\Documents\Ts Profiles Primary	1
Doug M. Bollinger	cf053f42-62a6-	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\Doug	C:\Users\Public\Documents\Ts Profiles	1
Douglas J. Hondo	1e390e30-4690	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\Douglas	C:\Users\Public\Documents\Ts Profiles	0
Francois DuPlesis	7c266ff5-9815-	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\Franc	C:\Users\Public\Documents\Ts Profiles Primary	0
Frederick K. Williams	f61192d4-7536	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\Fred	C:\Users\Public\Documents\Ts Profiles	0
Jordi j. alba	aa1195d8-9224	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\jordi	C:\Users\Public\Documents\Ts Profiles Primary	0
Marlon Samuels	14a4b1db-d1e1	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\Marlon	C:\Users\Public\Documents\Ts Profiles	1
Pat y. Symcox	a71e7857-3a20	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\pat	C:\Users\Public\Documents\Ts Profiles Primary	0
Shane Bond	328b68e3-cd28	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\shane	C:\Users\Public\Documents\Ts Profiles Primary	1
Tony J. Stark	1c7ea288-237e	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\Tony	C:\Users\Public\Documents\Ts Profiles Primary	1
Totti J. Alberto	f4f5e703-1eee-	S-1-5-21-18057	treelab.local/ADC_W	\\vssshares\TSprofilepaths\totti	C:\Users\Public\Documents\Ts Profiles Primary	1

Chapter 14

14 Power Export

14.1 About Power Export

ARKAD provides a powerful offline report generation tool called ***Power Export***. Power Export allows the user to select *multiple reports* to be run for a domain at scheduled intervals. The Power Export tool has the ability to *export and/or e-mail* the reports in different file formats.

Please note the following while using the Power Export Wizard:

a) *Scheduled reports* will be created as a *"task"* in Windows Task Scheduler.

b) The scheduled job will *generate* and *export/email* the reports in *different file formats* (HTML, CSV & XLSX) to the desired folder path.

c) By default, for each task, a sub-folder with the task name will be created under the specified export path. All selected Reports will be *exported* to a *time-stamped* sub-folder, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. Therefore, the full folder path for all the exported reports refers to the following directory: ***<Export path><Task name><Time stamp>.***
However, please note that the user can modify this default behaviour and have all the reports exported to the specified folder instead of the time-stamped sub-folder.

d) A *separate file* will be created *for each report* in the *desired file format*. For example, in the *HTML file format*, each report will be created as an *.html file.*

NOTE: ARKAD Power Export Wizard will help you create and store the settings for a task, which you may view or modify later using the Scheduled Tasks Manager. The task will be created with the settings (Schedule Type and Run As parameter) provided using the Power Export Wizard. A valid password must be specified for the Run As parameter of the task.

CHAPTER -13 –Power Exports

Using the ***Power Export Tool*** you can schedule the following reports:

- ***Object Reports***
- ***Built-in Object Reports***
- ***Built-in Security Reports***
- ***Forest Reports***
- ***Permissions Reports***
- ***Custom Reports***
- ***Custom LDAP Queries Reports***
- ***AD Summary Reports***
- ***Quick Reports***
- ***Terminal Services Reports***

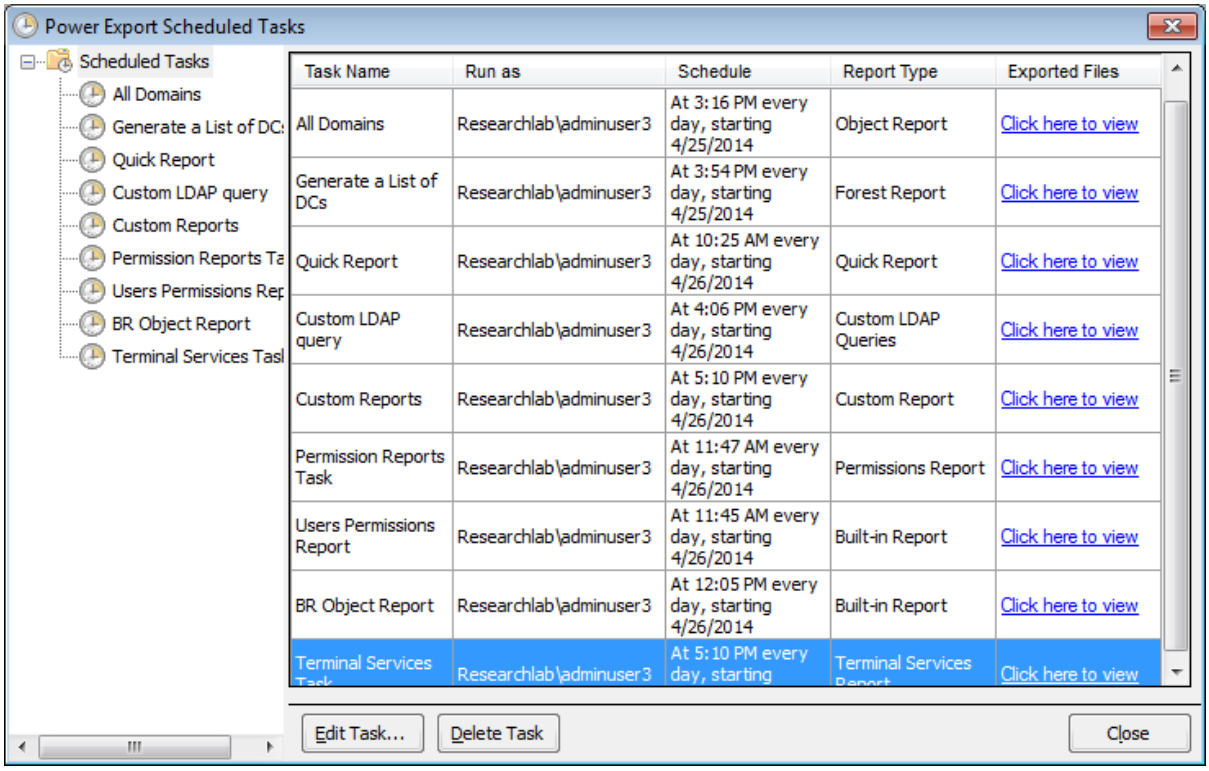
14.2 Scheduled Tasks Manager

The ***Scheduled Tasks Manager*** allows you to perform the following operations:

- ***View*** summary information for the tasks created
- ***View*** exported files of the task
- ***Edit*** an existing task
- ***Delete*** a task

View summary information of a task

The pane on the left hand side in the Scheduled Tasks Manager window lists the tasks maintained in ARKAD. To view summary information of a task, select the desired task on the left pane. The summary information of the selected task will be displayed in the right pane as shown below:



The *task summary* includes information about the *task, reports selected, export/e-mail settings.*

View exported files

To view the reports generated and exported by the task, perform either one of the following steps:

- Select ***Scheduled Tasks*** node on the left pane, and then click on the hyperlink in the ***Exported Files*** column in the right pane for the desired task.

- ***OR***

- *Select* the desired task on the left pane, and then click on the hyperlink next to ***Exported Files.***

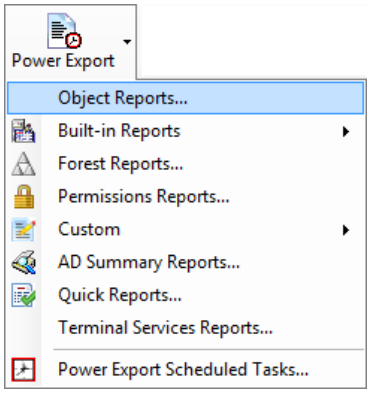
Edit Task

1) *Select a task* from the Scheduled Tasks Manager Window and Click ***Edit Task****.*
2) Perform the steps as outlined in Schedule Object Reports or Schedule Custom Reports based on the scheduled report type. While proceeding through the wizard you may change the settings, add a new report, delete a report, edit a report, change the export path etc.,
3) The new settings will be used when the task runs the next time.

Delete Task

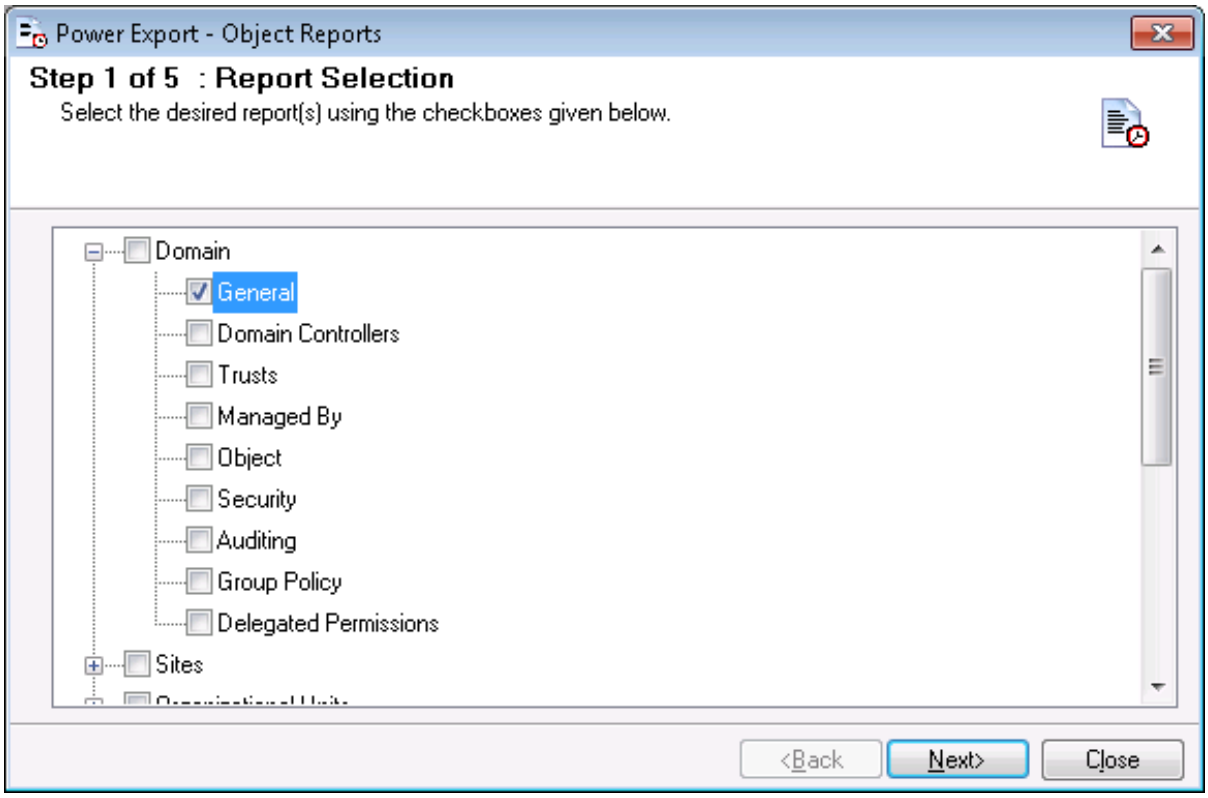
To *delete* a task from the Scheduled Task Manager, select the task and Click ***Delete Task.*** The deleted task will be removed *permanently* from the Windows Task Scheduler.

14.3 Schedule Object Reports



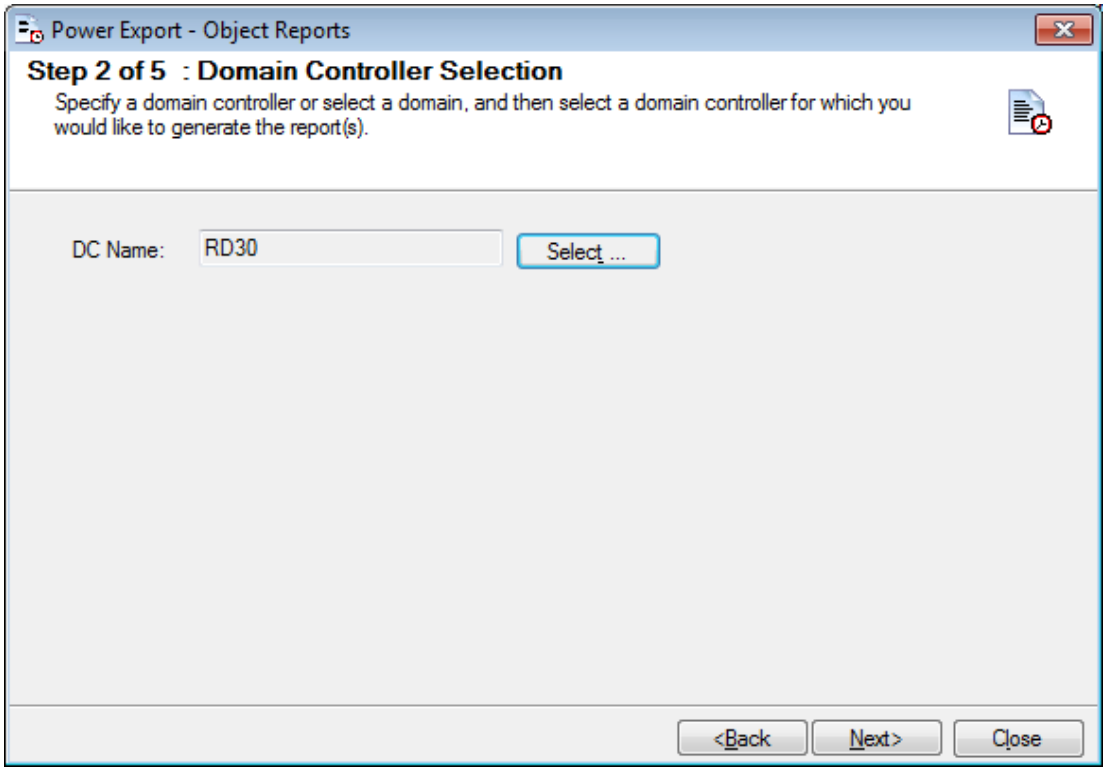
Select *option* under *Power Export.* This will bring up the *Power Export Wizard.*

Step 1: Report Selection



1) ***Select*** the report(s) using the ***checkboxes*** to the left of the reports. You may select any number of reports to run in a single task.
2) *Click* ***Next*** to proceed to the next step. You may *Click Back* button anytime to come back to a previous step.

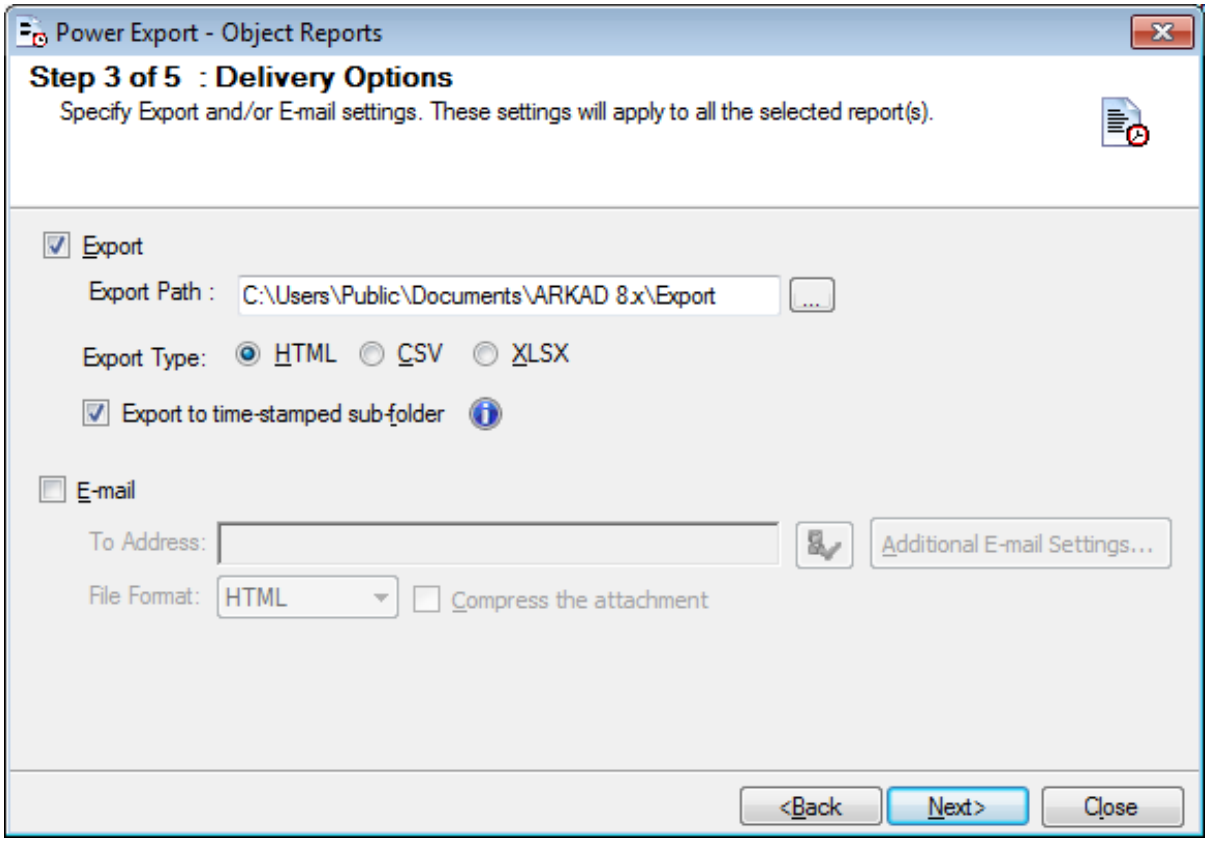
Step 2: Domain Controller Selection


Power Export - Object Reports
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) Specify a domain controller for which you want to generate the selected custom report. Click *Select button* to specify a domain controller. The Connection Manager will be displayed which will allow you to specify a domain controller

2) *Click* ***Next*** to proceed to the next Step.

Step 3: Export/Email Options



1) Change the ***Export or Email*** settings as necessary.

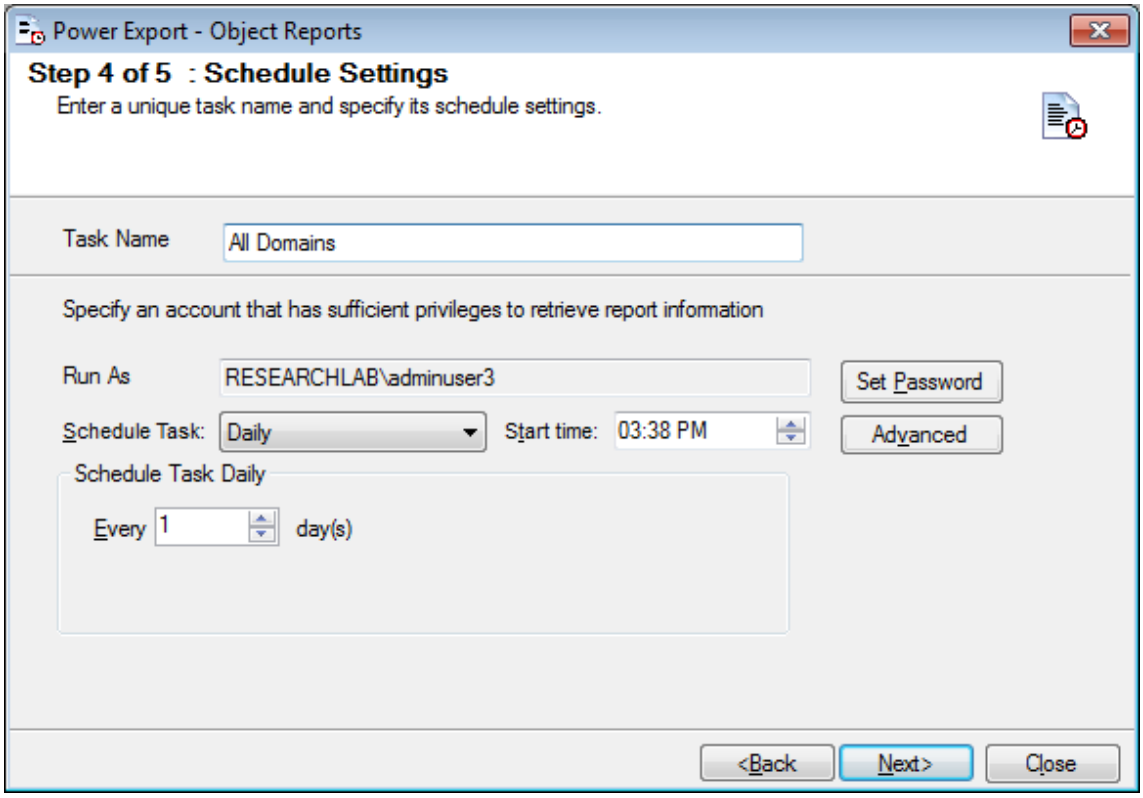
2) Use ***Browse button*** to change the ***export path*.**

3) The *export path* refers to the *destination location* where the output file generated should be stored. By default, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear ***"Export to time-stamped sub-folder"*** option.

NOTE: Clearing the "Export to time-stamped sub-folder" option will overwrite existing files, if any, in the specified export path.

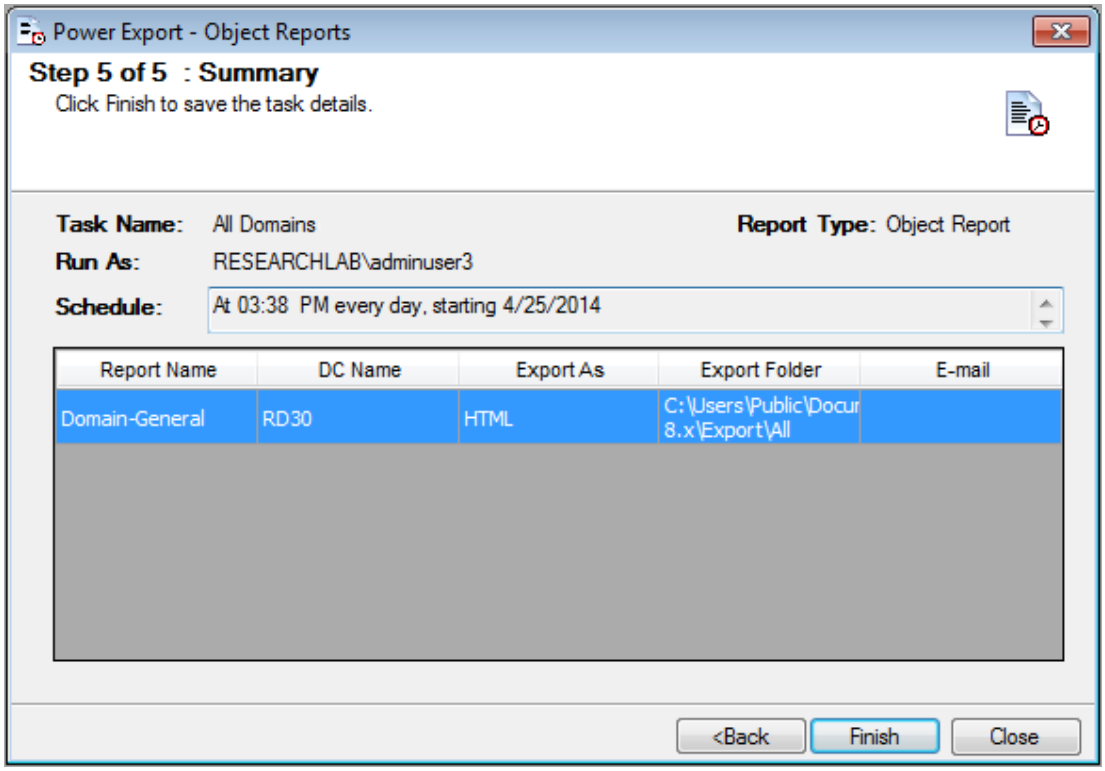
4) *Click* ***Next*** to proceed to the next step.

Step 4: Schedule Settings



1) *Enter* a ***unique name*** for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click* ***Next*** to proceed to the next and final step.

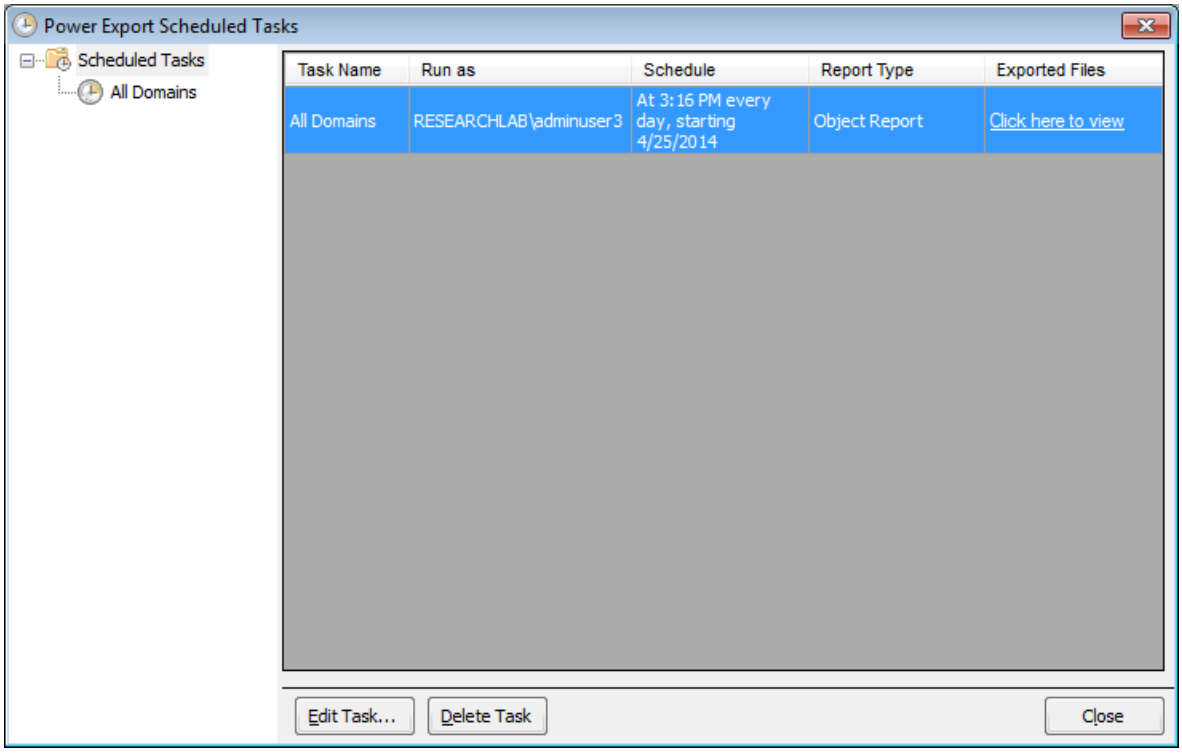
Step 5: Summary



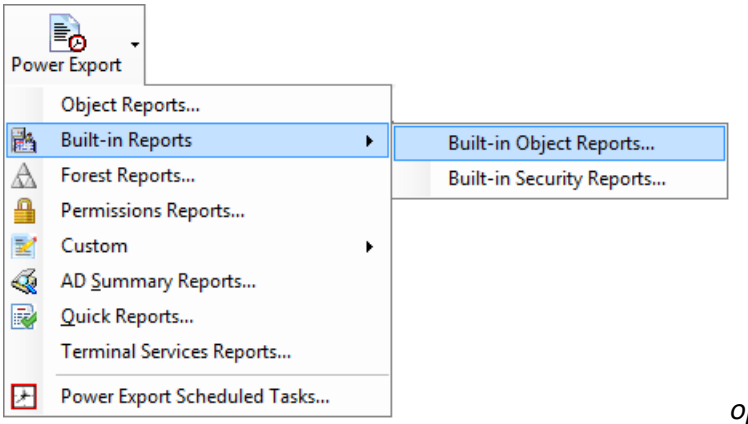
1) This step displays the *summary information* of the task.

2) Click ***Finish*** to save the task details.

3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:



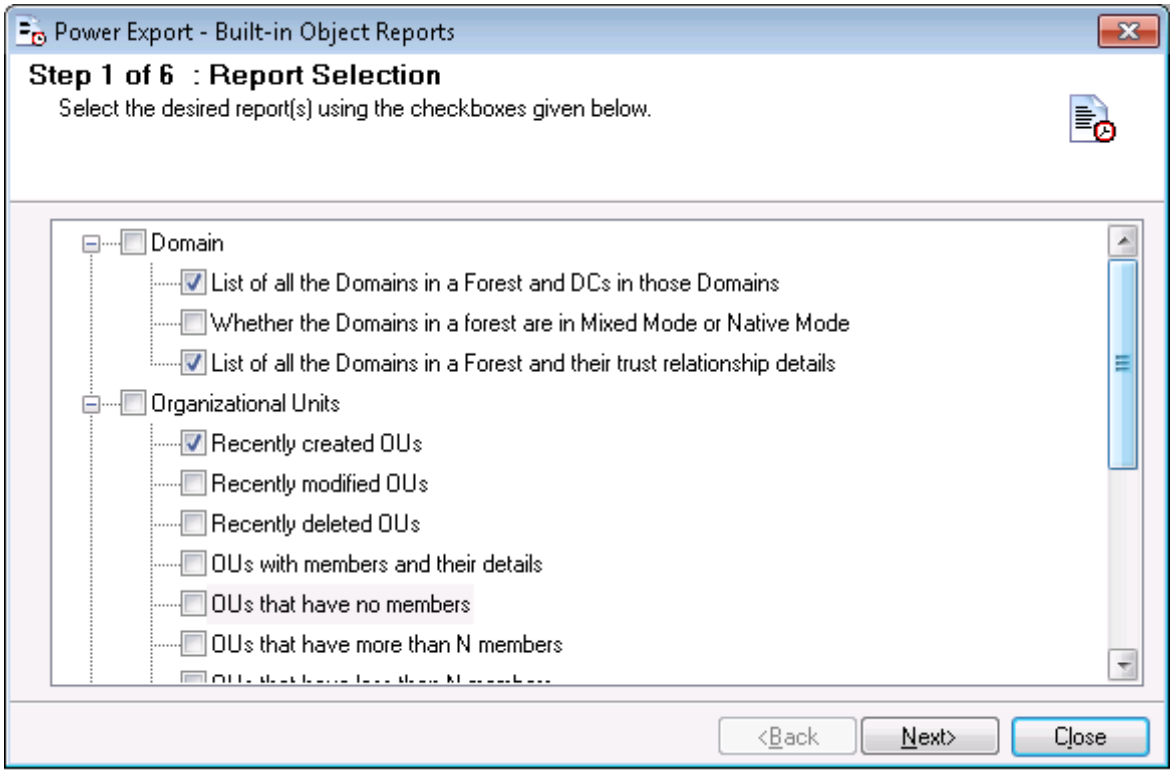
14.4 Schedule Built-in Object Reports



Select *option* under *Power Export.*

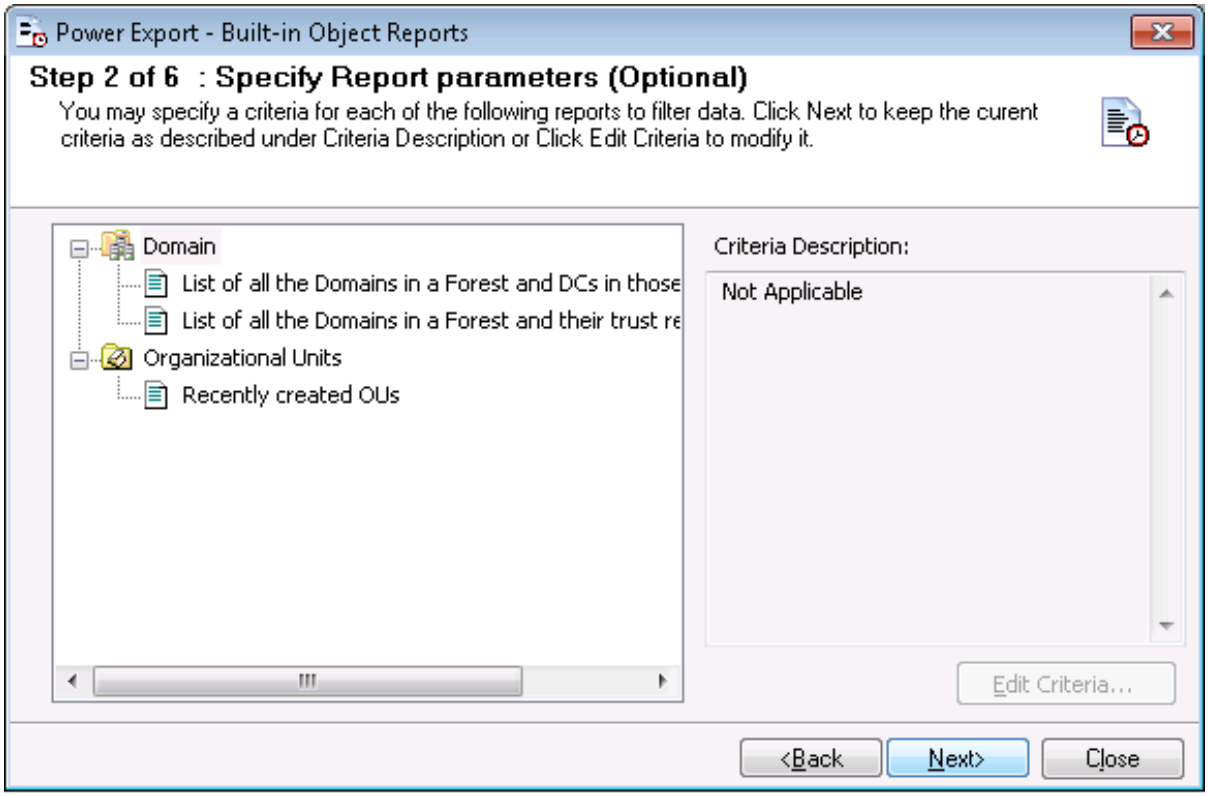
This will bring up the *Power Export* Wizard.

Step 1: Report Selection

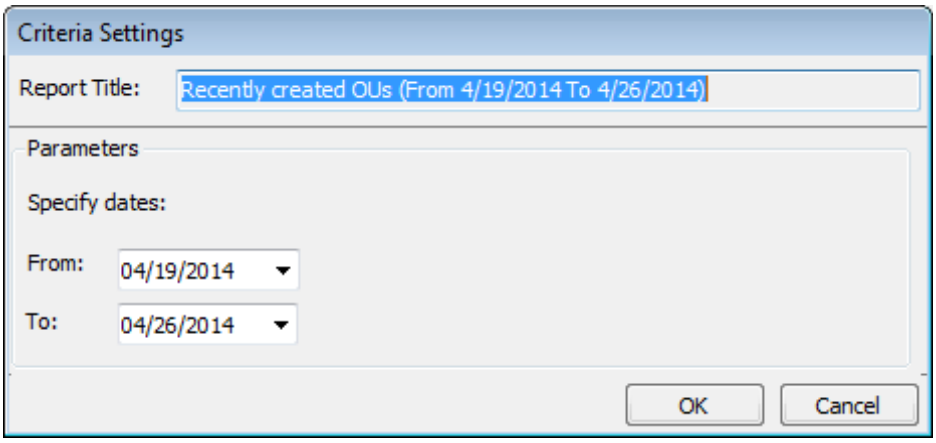

Power Export - Built-in Object Reports
Step 1 of 6 : Report Selection
Select the desired report(s) using the checkboxes given below.
Domain
List of all the Domains in a Forest and DCs in those Domains
Whether the Domains in a forest are in Mixed Mode or Native Mode
List of all the Domains in a Forest and their trust relationship details
Organizational Units
Recently created OUs
Recently modified OUs
Recently deleted OUs
OUs with members and their details
OUs that have no members
OUs that have more than N members
<Back
Next>
Close

1) *Select* the report(s) using the *checkboxes* to the left of the reports. You may select any number of reports to run in a single task.
2) *Click* ***Next*** to proceed to the next step. You may *Click* ***Back*** button anytime to come back to a previous step.

Step 2: Specify Report Parameters (Optional)

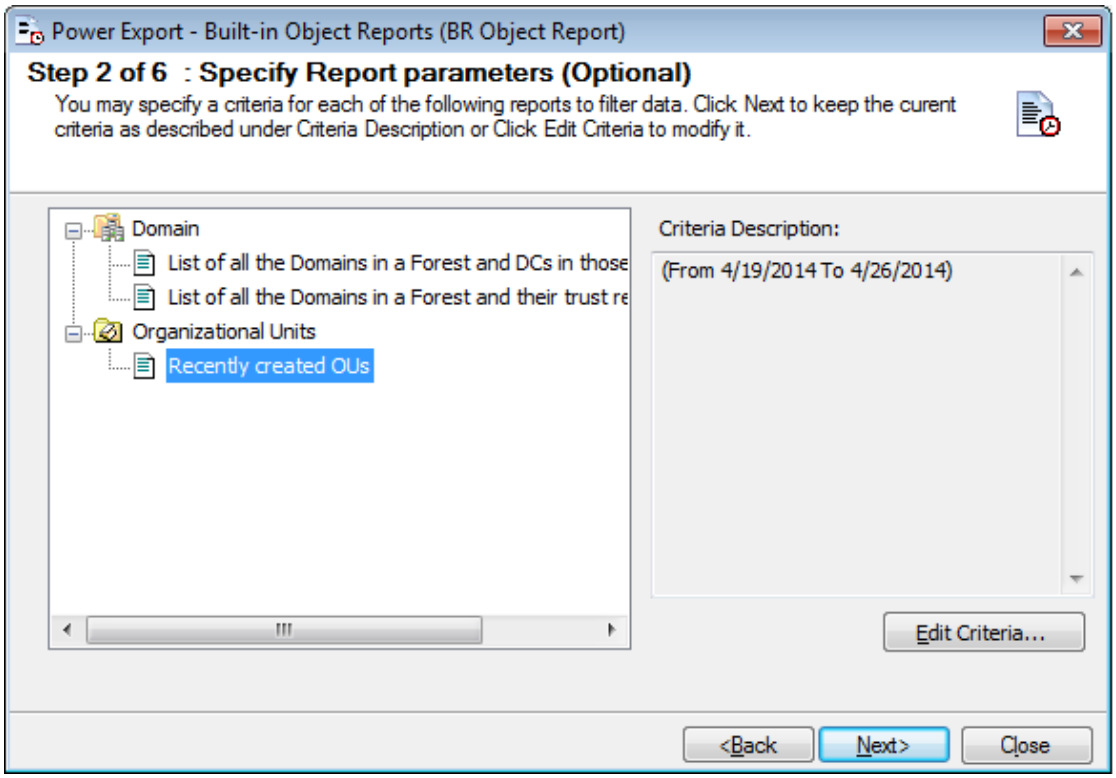

Power Export - Built-in Object Reports
Step 2 of 6 : Specify Report parameters (Optional)
You may specify a criteria for each of the following reports to filter data. Click Next to keep the curent criteria as described under Criteria Description or Click Edit Criteria to modify it.
Domain
List of all the Domains in a Forest and DCs in those
List of all the Domains in a Forest and their trust re
Organizational Units
Recently created OUs
Criteria Description:
Not Applicable
Edit Criteria...
<Back
Next>
Close

1) You can modify parameters of the selected report(s) by clicking on **Edit Criteria....** The **Criteria Settings** dialog would be displayed as shown below:



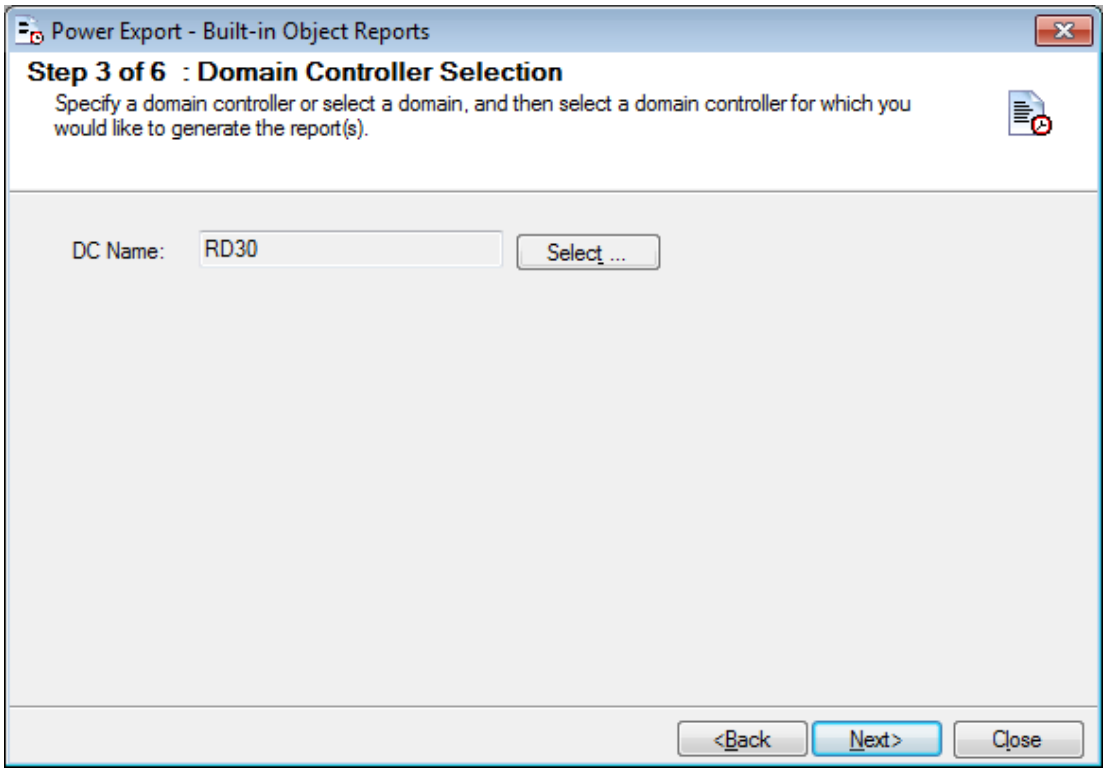
2) Modify the **parameters** and *click* **OK.**

3) A description of the selected criteria will be displayed under **Criteria Description** as shown below:


Power Export - Built-in Object Reports (BR Object Report)
Step 2 of 6 : Specify Report parameters (Optional)
You may specify a criteria for each of the following reports to filter data. Click Next to keep the curent criteria as described under Criteria Description or Click Edit Criteria to modify it.
Domain
List of all the Domains in a Forest and DCs in those
List of all the Domains in a Forest and their trust re
Organizational Units
Recently created OUs
Criteria Description:
(From 4/19/2014 To 4/26/2014)
Edit Criteria...
<Back
Next>
Close

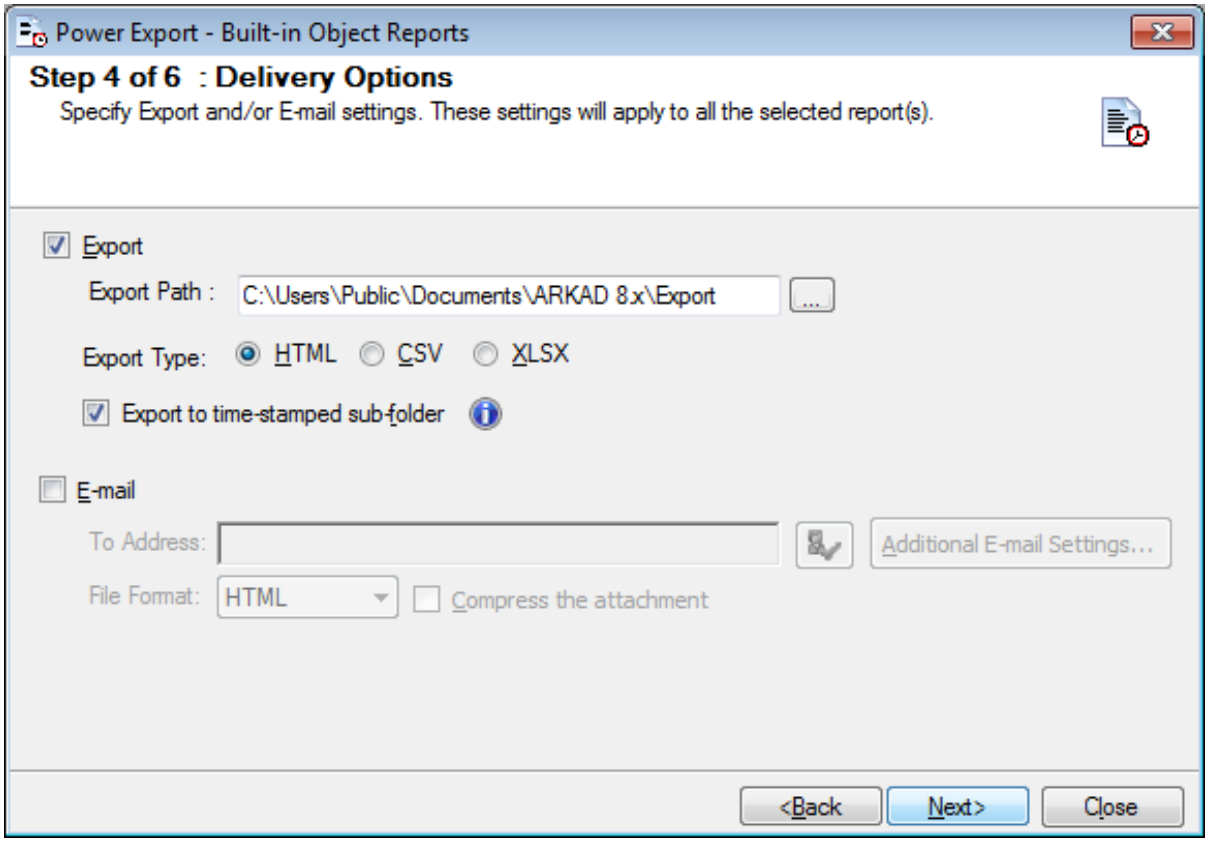
4) *Click **Next*** to proceed to the *Next* step.

Step 3: Domain Controller Selection


Power Export - Built-in Object Reports
Step 3 of 6 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) Specify a domain controller for which you want to generate the selected custom report. *Click* ***Select*** button to specify a **domain controller**. The Connection Manager will be displayed which will allow you to specify a domain controller
2) *Click* ***Next*** to proceed to the *nex*t Step.

Step 4: Export/Email Options

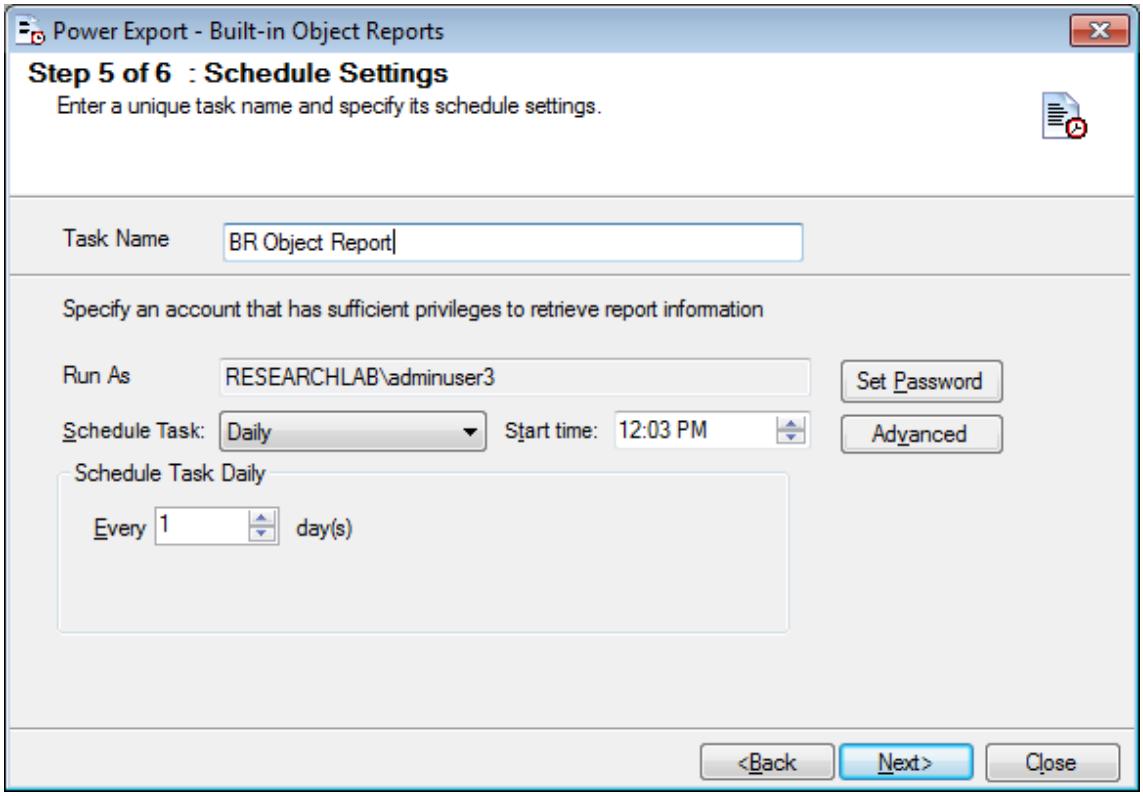


1) Change the **Export** or **Email** settings as necessary.
2) Use **Browse button** to change the export path.
3) The **export path** refers to the **destination location** where the output file generated should be stored. By default, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear **"Export to time-stamped sub-folder"** option.

   NOTE: Clearing the "Export to time-stamped sub-folder" option will overwrite existing files, if any, in the specified export path.

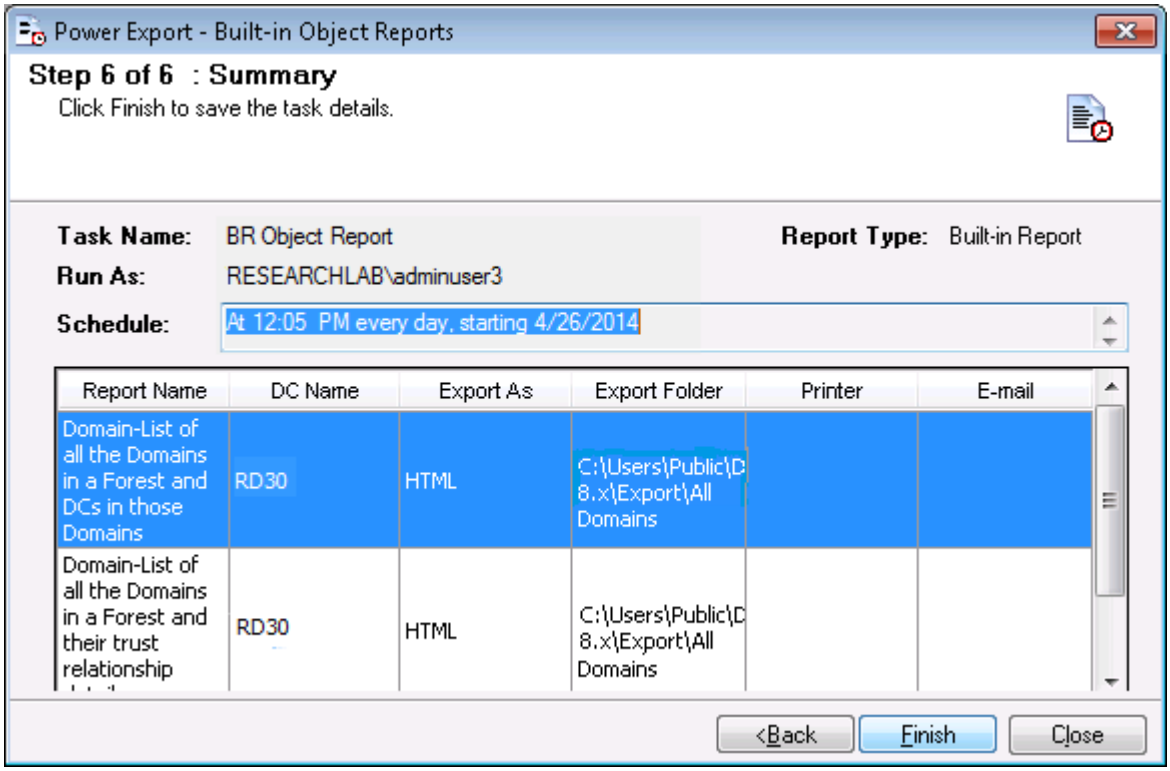
3) *Click* ***Next*** to proceed to the next step.

Step 5: Schedule Settings



1) *Enter* a **unique name** for the task.
2) *Change* the **Run as** parameter, if necessary and **set the password** for the specified user.
3) *Change t*he **task schedule** settings as required.
4) *Click* ***Next*** to proceed to *the next* and final step.

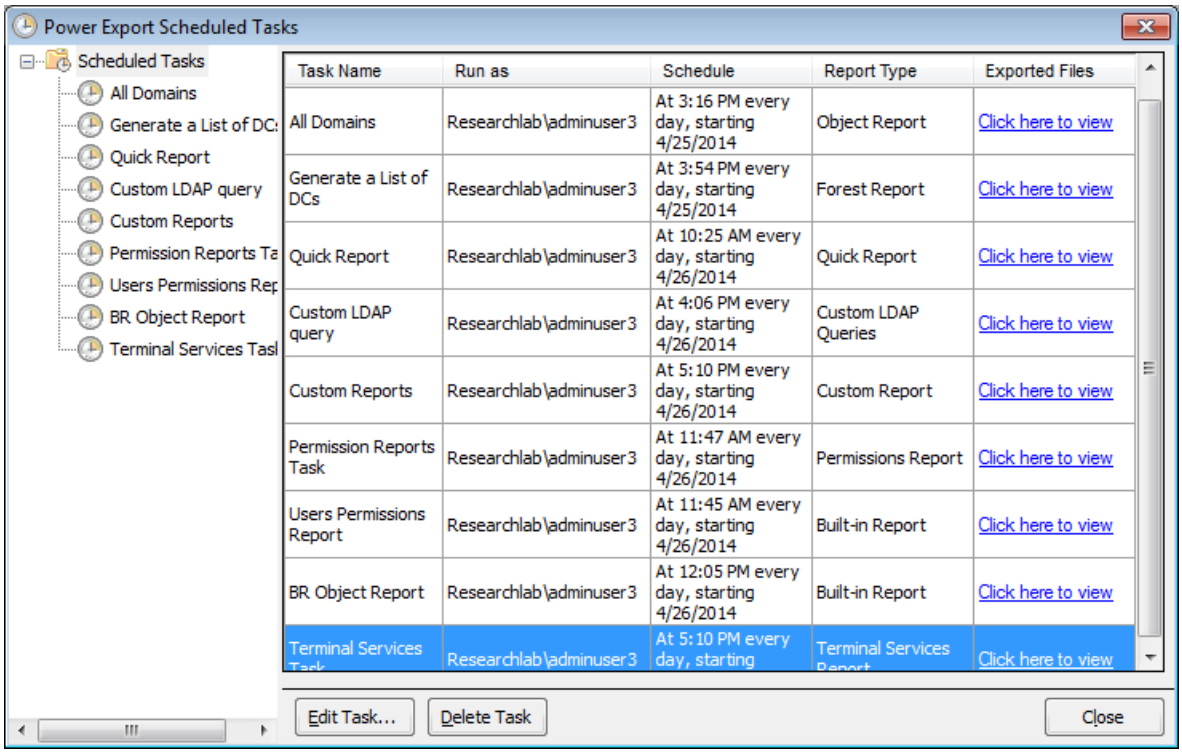
Step 6: Summary



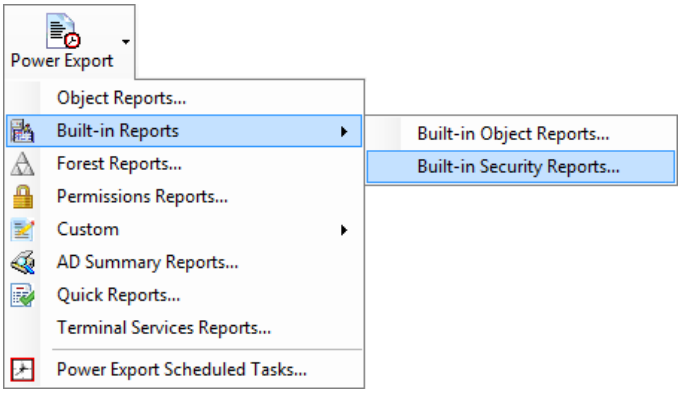
1) This step displays the **summary information** of the task.

2) *Click **Finish*** to save the task details.

3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:



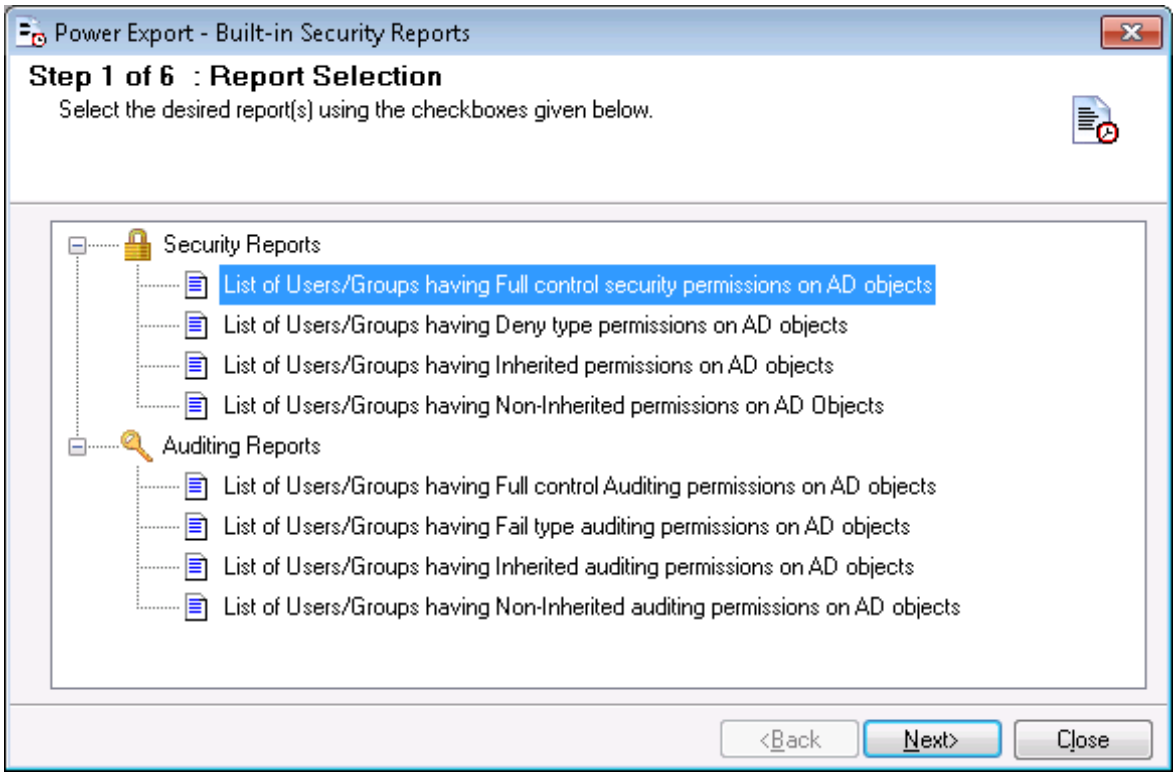
14.5 Schedule Built-in Security Reports



Select *option* under *Power Export*.

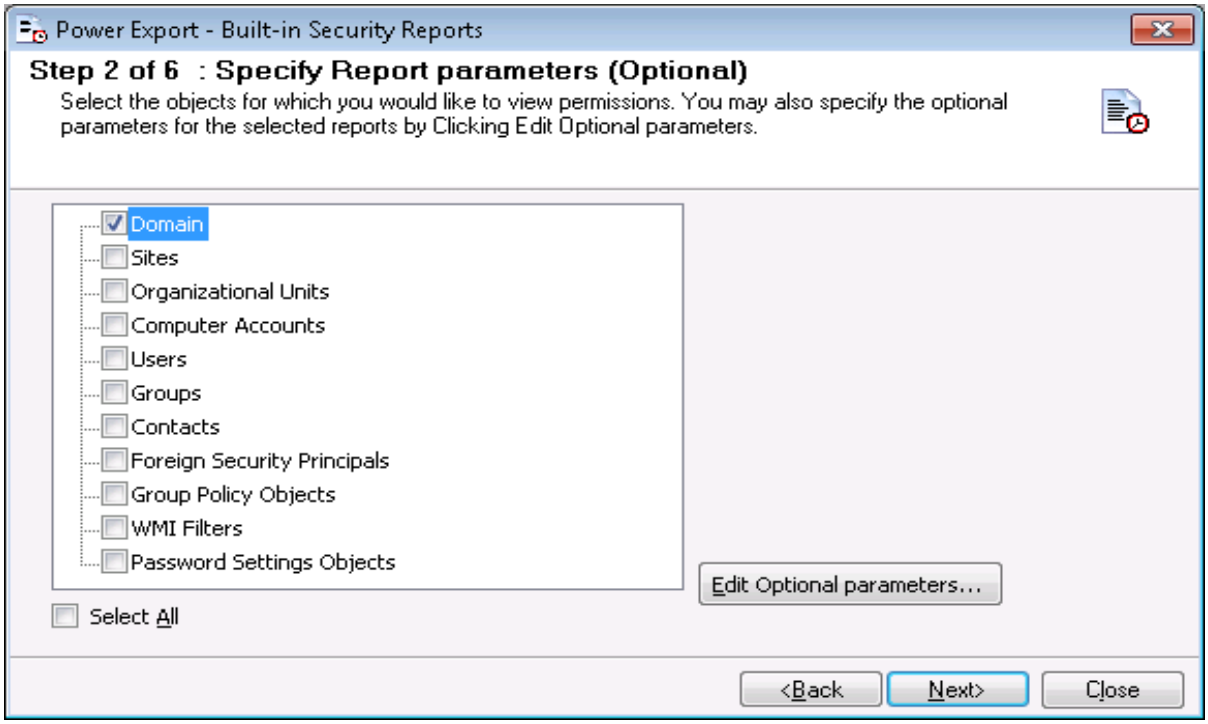
This will bring up the ***Power Export*** *Wizard.*

Step 1: Report Selection


Power Export - Built-in Security Reports
Step 1 of 6 : Report Selection
Select the desired report(s) using the checkboxes given below.
Security Reports
List of Users/Groups having Full control security permissions on AD objects
List of Users/Groups having Deny type permissions on AD objects
List of Users/Groups having Inherited permissions on AD objects
List of Users/Groups having Non-Inherited permissions on AD Objects
Auditing Reports
List of Users/Groups having Full control Auditing permissions on AD objects
List of Users/Groups having Fail type auditing permissions on AD objects
List of Users/Groups having Inherited auditing permissions on AD objects
List of Users/Groups having Non-Inherited auditing permissions on AD objects
<Back
Next>
Close

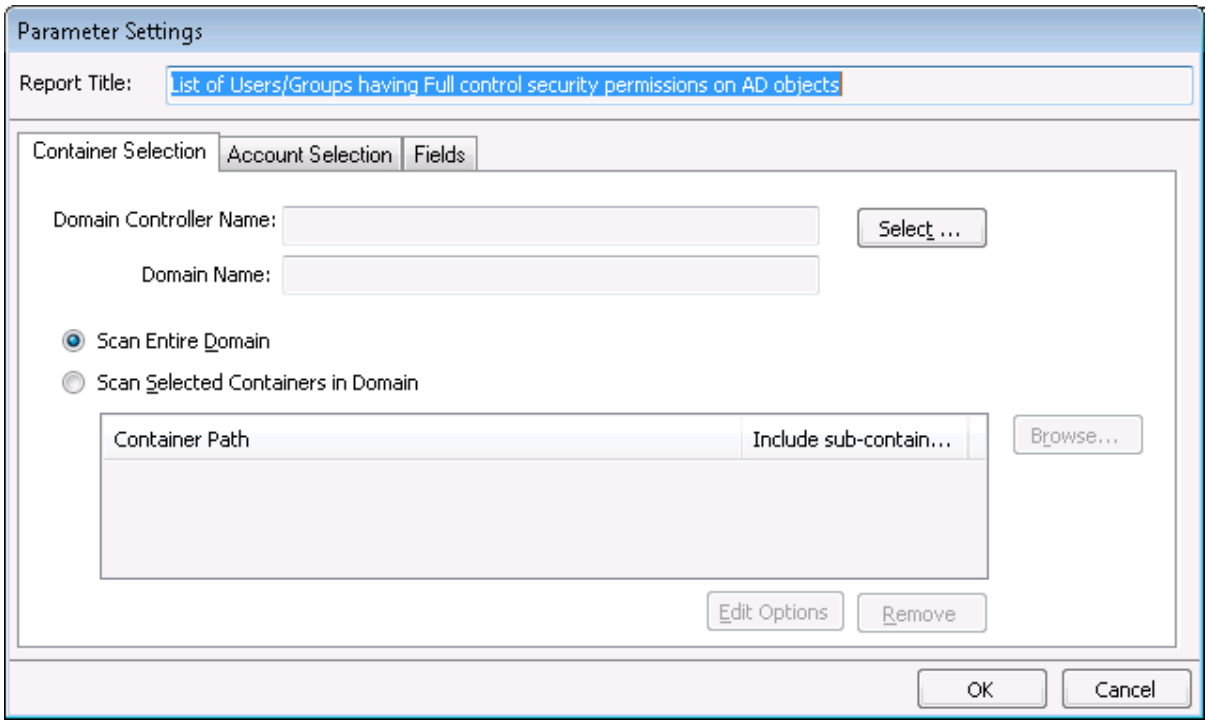
1) ***Select*** the desired report. Only one report may be selected to run in a single task.
2) *Click* ***Next*** to proceed to the next step. You may *Click Back* button anytime to come back to a previous step.

Step 2: Specify Report Parameters (Optional)

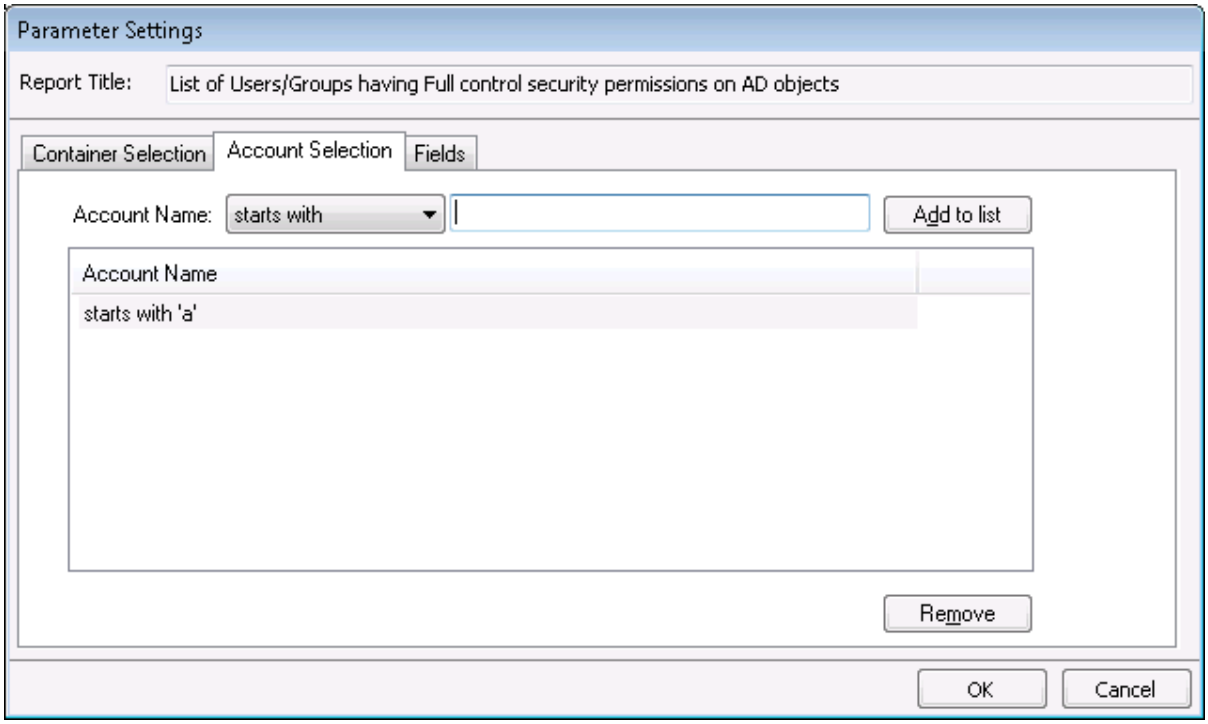

Power Export - Built-in Security Reports
Step 2 of 6 : Specify Report parameters (Optional)
Select the objects for which you would like to view permissions. You may also specify the optional parameters for the selected reports by Clicking Edit Optional parameters.
Domain
Sites
Organizational Units
Computer Accounts
Users
Groups
Contacts
Foreign Security Principals
Group Policy Objects
WMI Filters
Password Settings Objects
Edit Optional parameters...
Select All
<Back
Next>
Close

1) ***Select*** the *objects* for which you would like to *view permissions.* You may also modify the optional parameters of the selected report by clicking on ***Edit Optional Parameters….*** The ***Parameter settings*** dialog would be displayed as shown below:

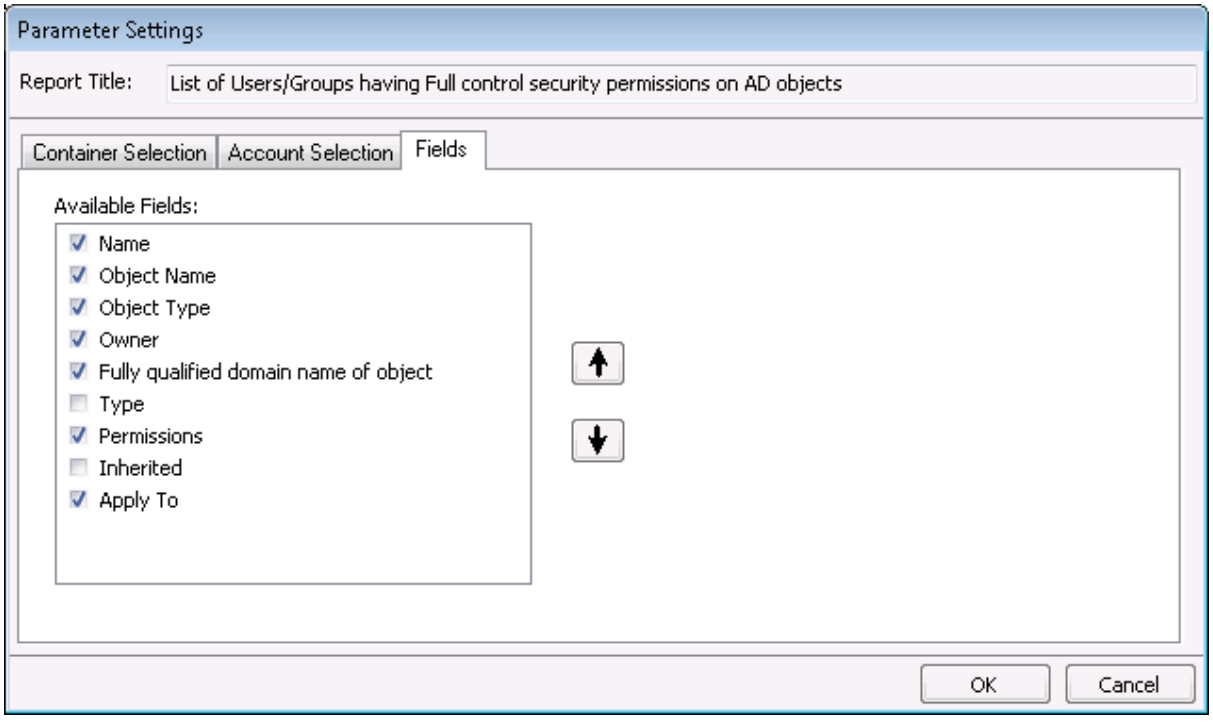
Container Selection



User/Group Accounts Selection

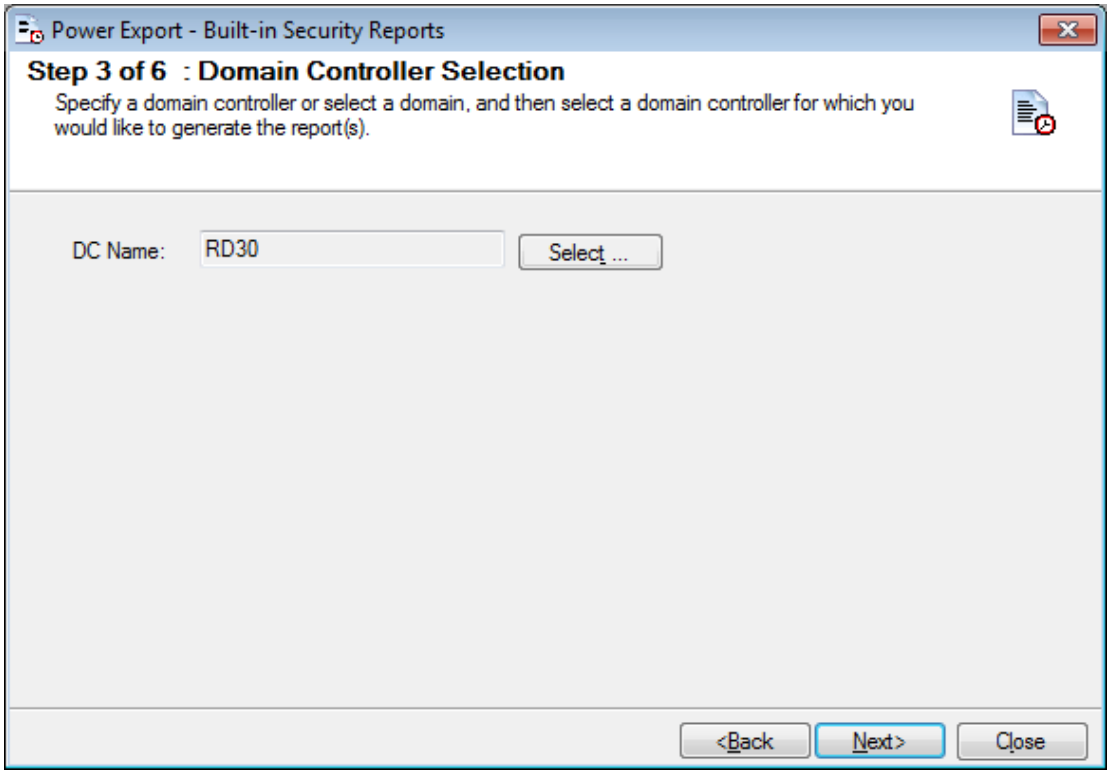


Field Selection



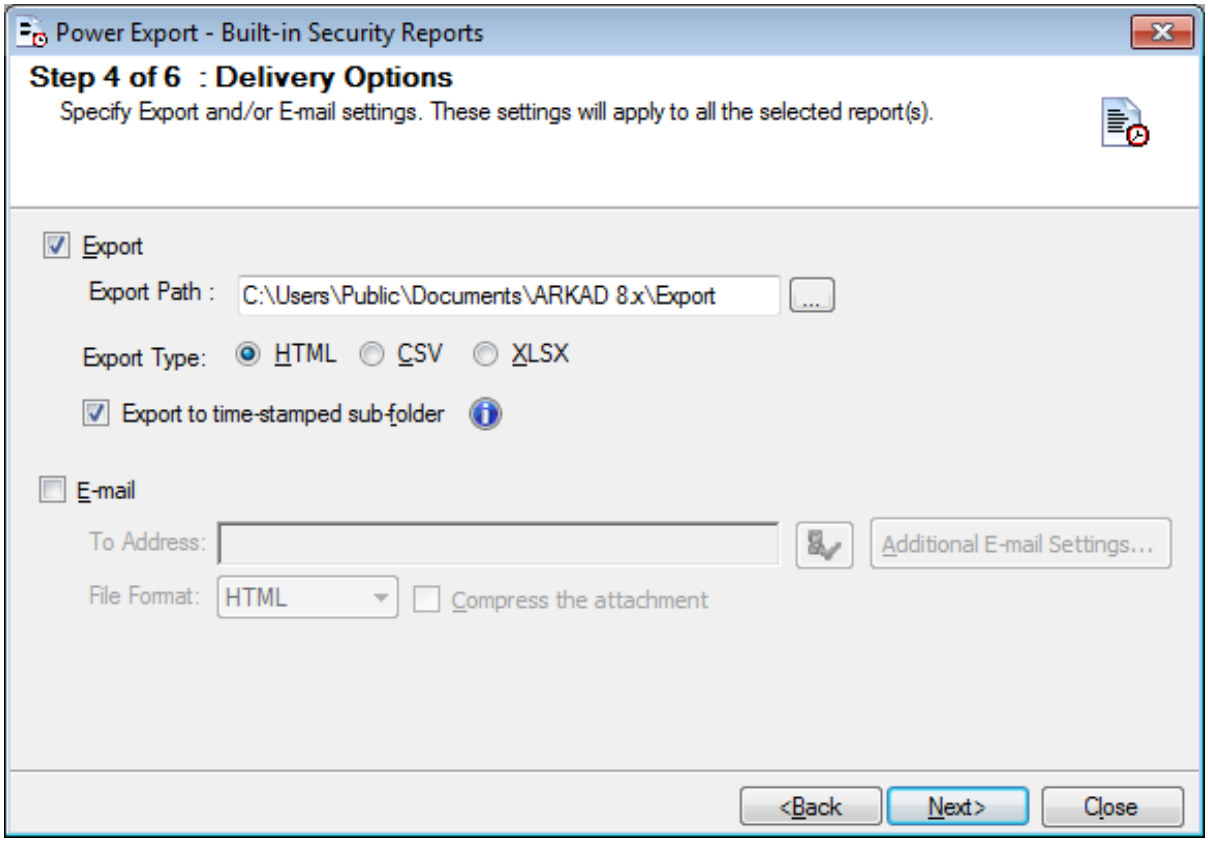
2) Modify the *parameters* and *click* ***OK*** to refresh the selected Built-in report.

Step 3: Domain Controller Selection


Power Export - Built-in Security Reports
Step 3 of 6 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) *Specify a domain controller for which you want to generate the selected custom report. Click* ***Select*** button to specify a ***domain controller***. The Connection Manager will be displayed which will allow you to specify a domain controller
2) *Click* ***Next*** to proceed to the next Step.

Step 4: Export/Email Options



1) Change the ***Export*** *or* ***Email*** settings as necessary.

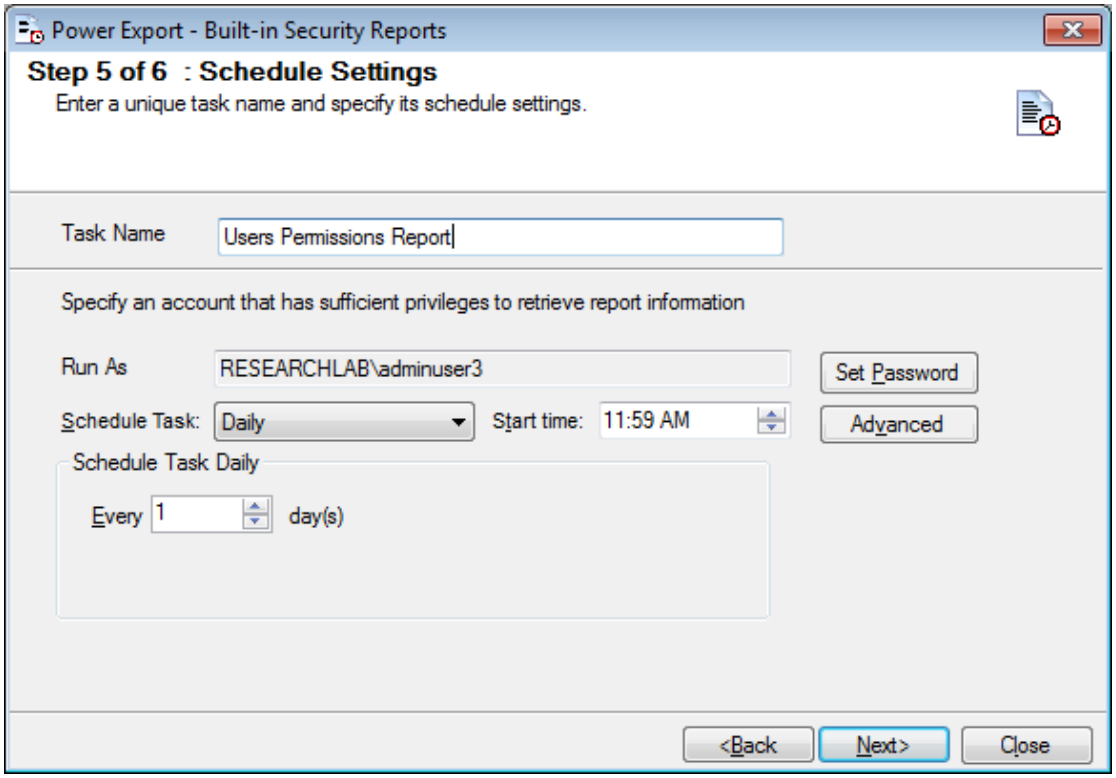
2) Use ***Browse*** button to change the export path.

3) The *export path* refers to the *destination location* where the output file generated should be stored. By *default*, for each task, a *sub-folder* with the task name will be created under the specified *export path.* All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear ***"Export to time-stamped sub-folder"*** option.

NOTE: Clearing the "Export to time-stamped sub-folder" option will overwrite existing files, if any, in the specified export path.

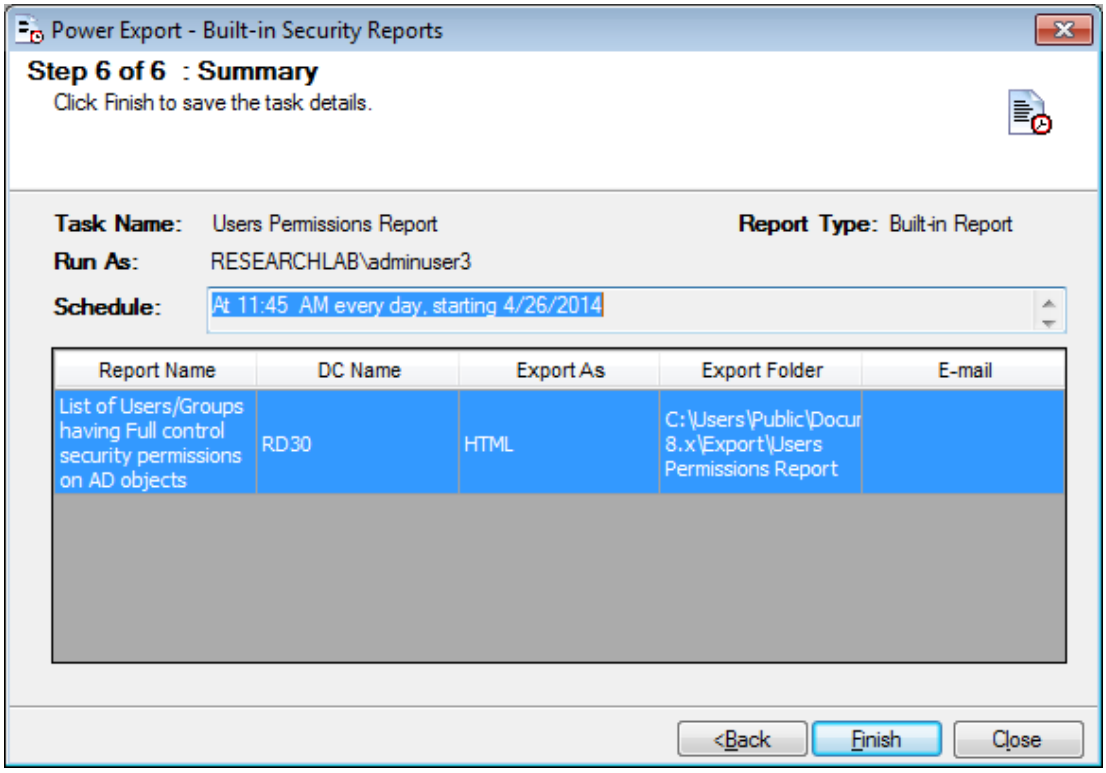
4) *Click* ***Next*** to proceed to the next step.

Step 5: Schedule Settings



1) *Enter* a ***unique*** name for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click* ***Next*** to proceed to the *nex*t and final step.

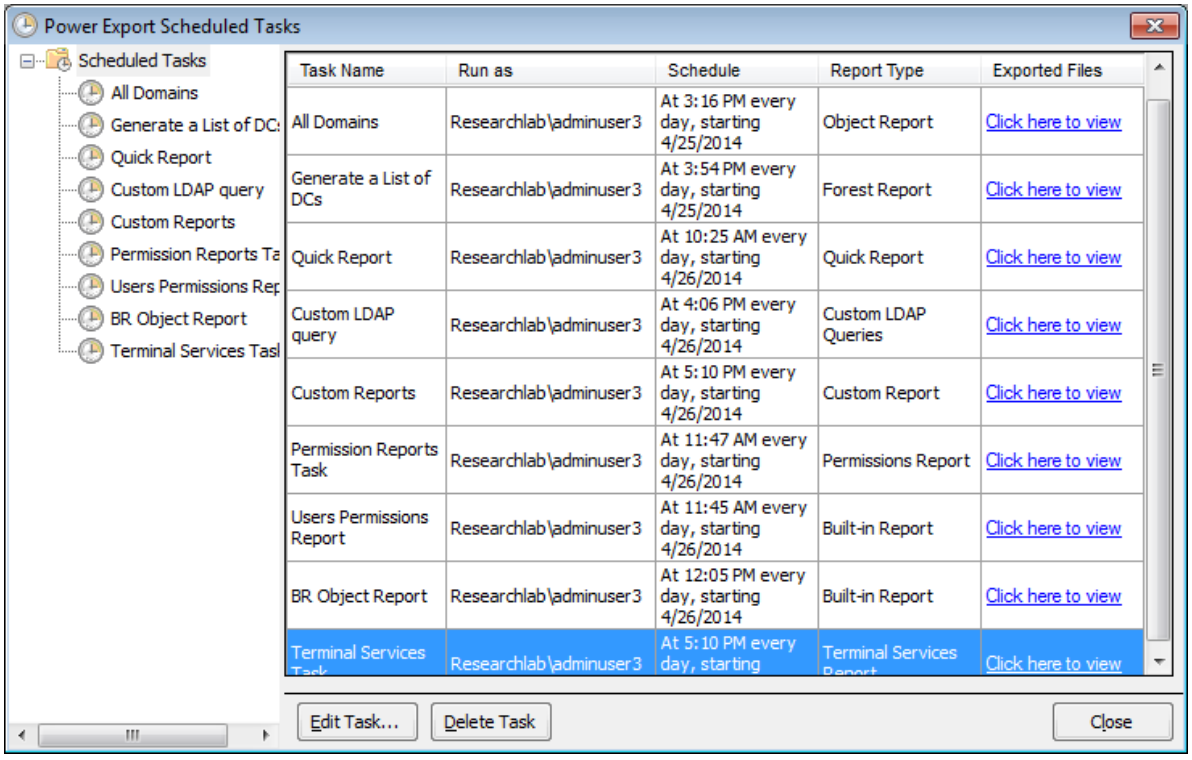
Step 6: Summary



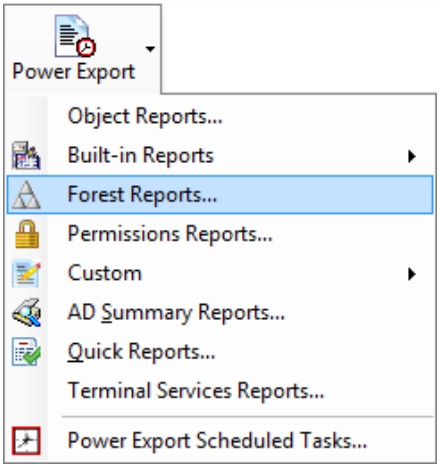
1) This step displays the ***summary*** *information* of the task.

2) *Click* ***Finish*** *to save* the task details.

3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:

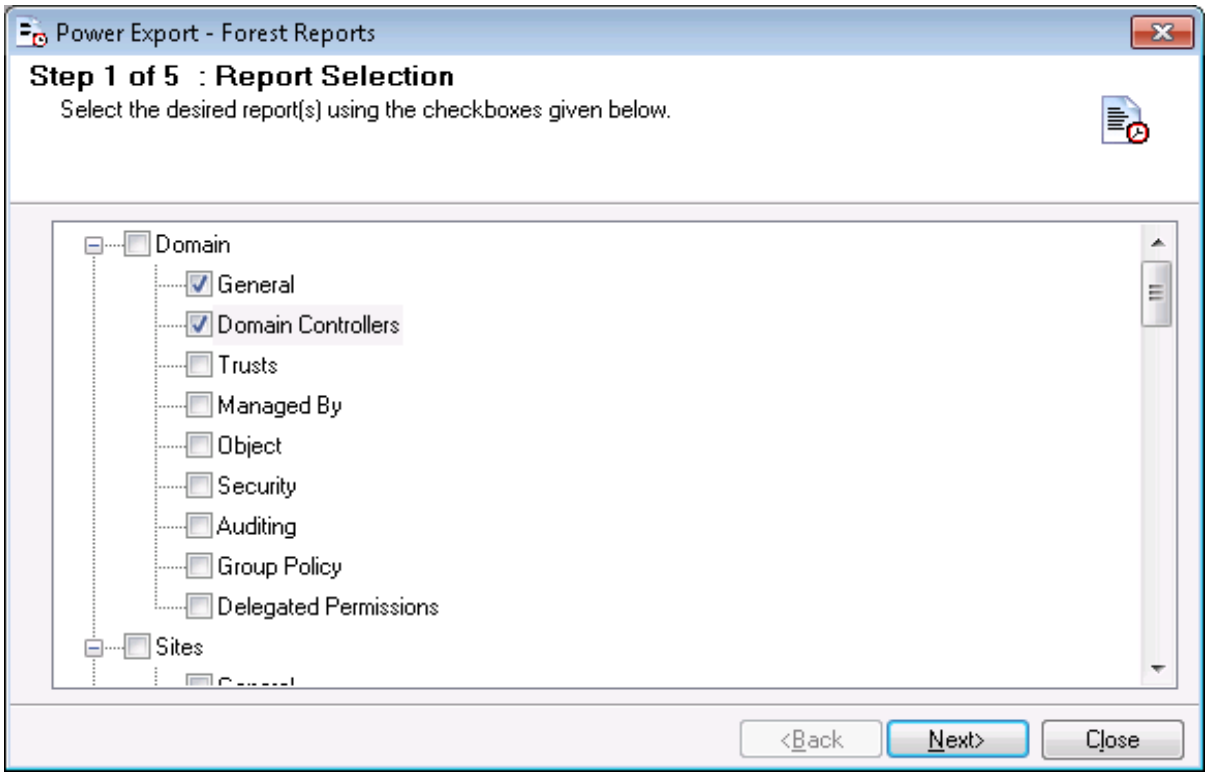


14.6 Schedule Forest Reports



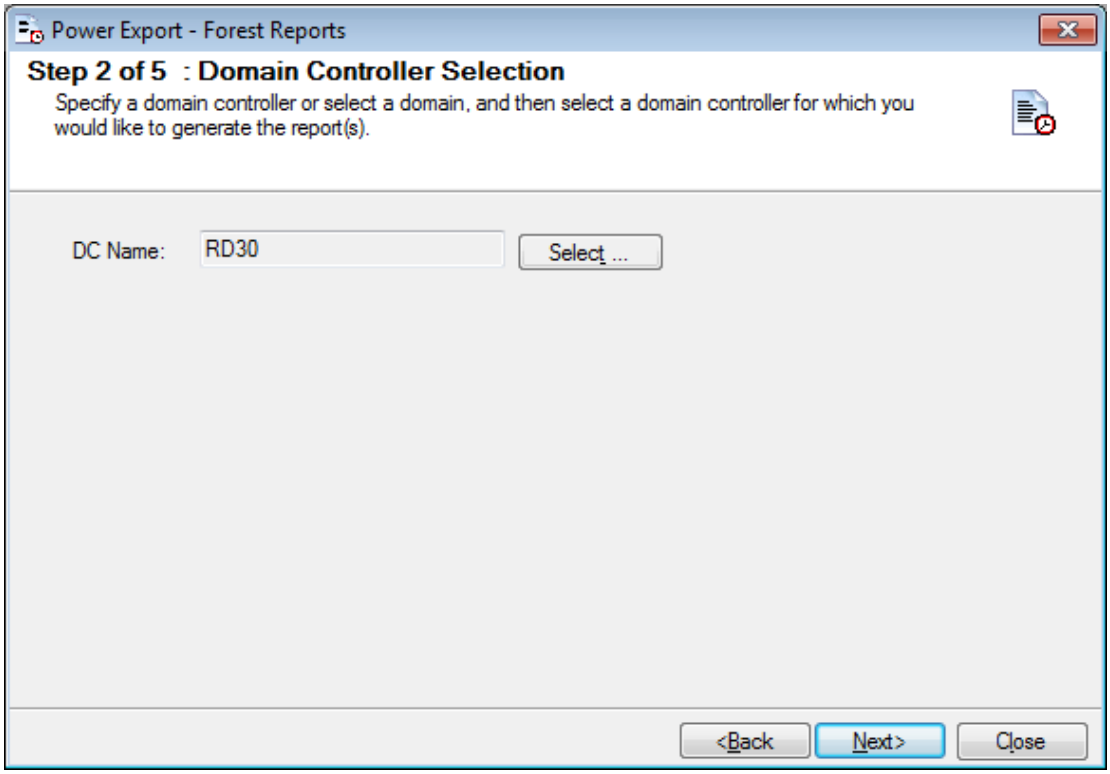
Select *option under Power Export.* This will bring up the ***Power Export*** *Wizard.*

Step 1: Report Selection



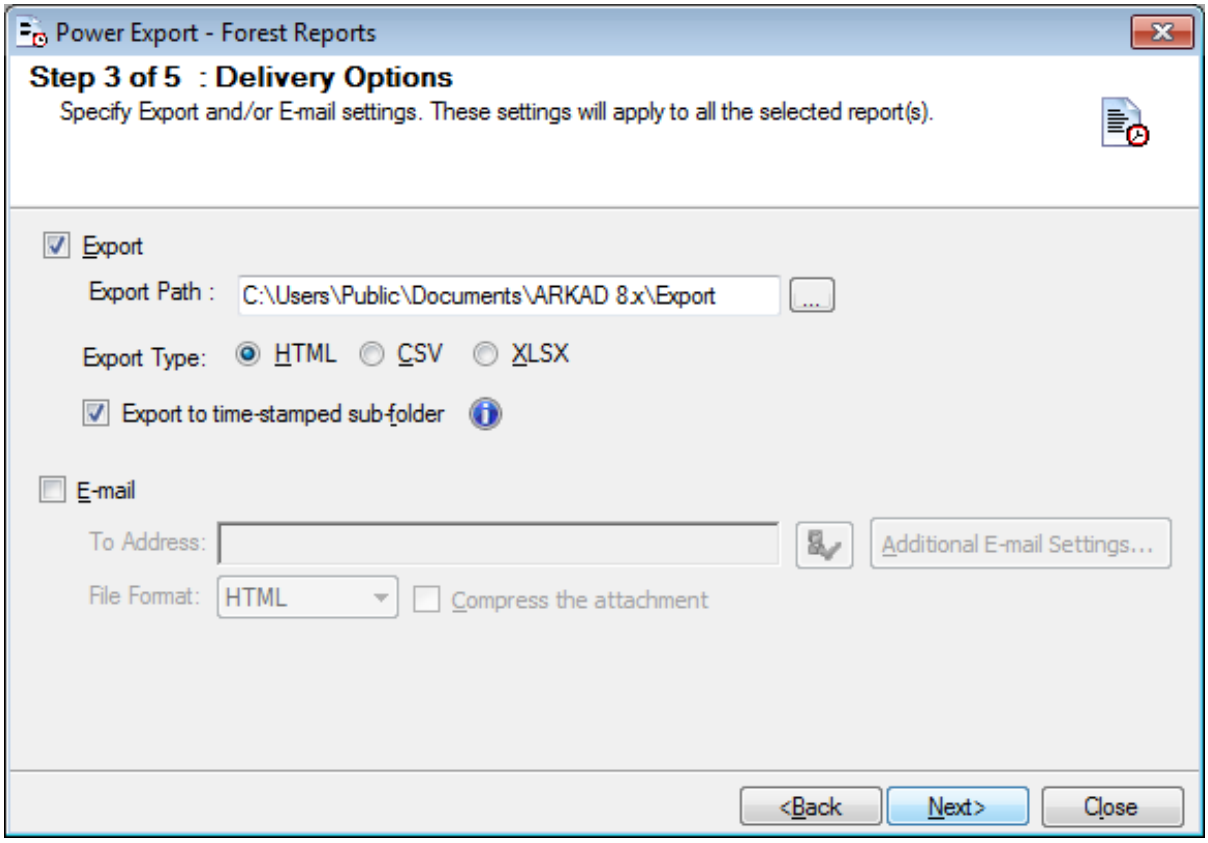
1) ***Select*** the report(s) using the ***checkboxes*** to the left of the reports. You may select any number of reports to run in a single task.
2) *Click* ***Next*** to proceed to the next step. You may *Click Back* button anytime to come back to a previous step.

Step 2: Domain Controller Selection


Power Export - Forest Reports
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) *Specify a domain controller for which you want to generate the selected custom report. Click* ***Select*** button to specify a domain controller. The Connection Manager will be displayed which will allow you to specify a domain controller.
2) *Click* ***Next*** to proceed to the next Step.

Step 3: Export/Email Options



1) *Change* the ***Export*** *or* ***Email*** settings as necessary.

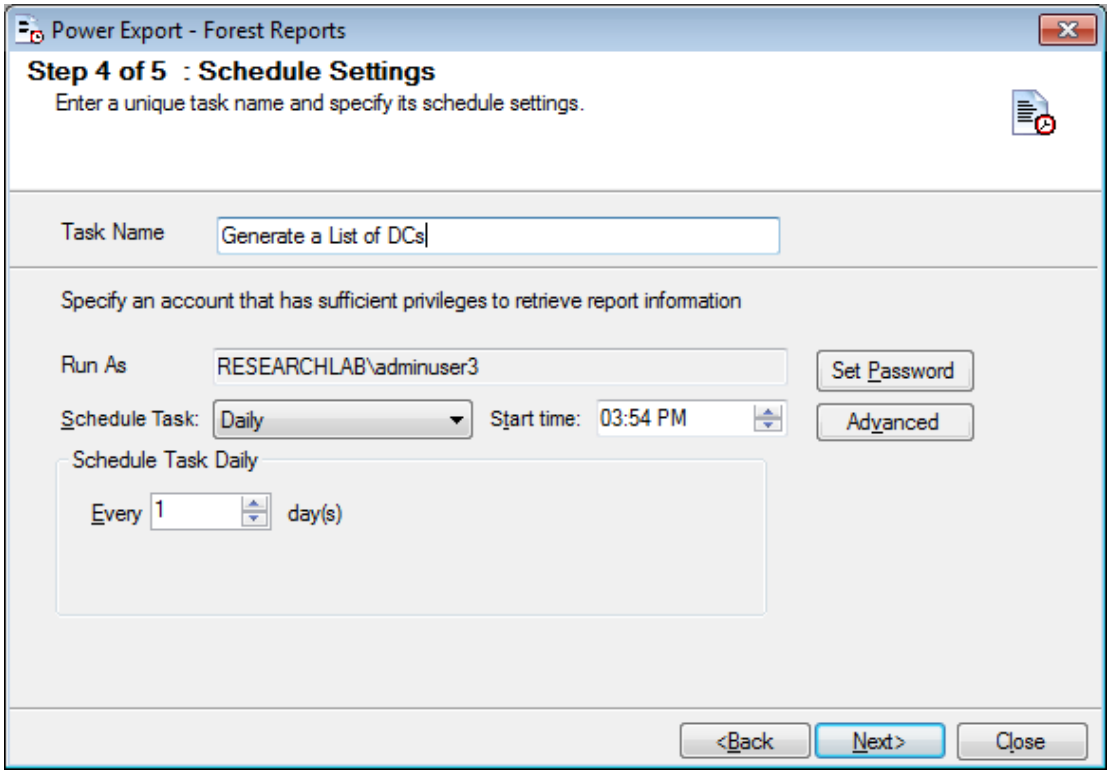
2) *Use* ***Browse*** button to change the ***export path.***

3) The ***export path*** refers to the *destination location* where the output file generated should be stored. By *default*, for each task, a *sub-folder* with the task name will be created under the specified export path. All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear ***"Export to time-stamped sub-folder"*** option.

NOTE: Clearing the "Export to time-stamped sub-folder" option will overwrite existing files, if any, in the specified export path.

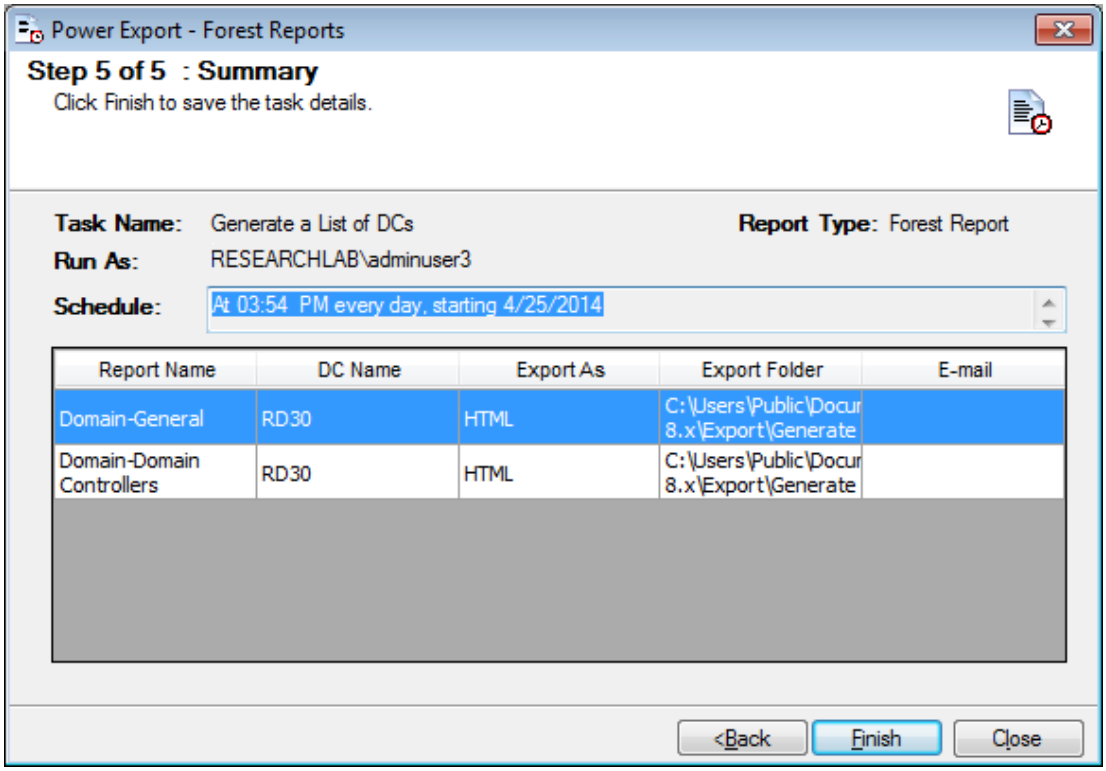
4) *Click* ***Next*** to proceed to the next step.

Step 4: Schedule Settings



1) *Enter* a ***unique name*** for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click* ***Next*** to proceed to the next and final step.

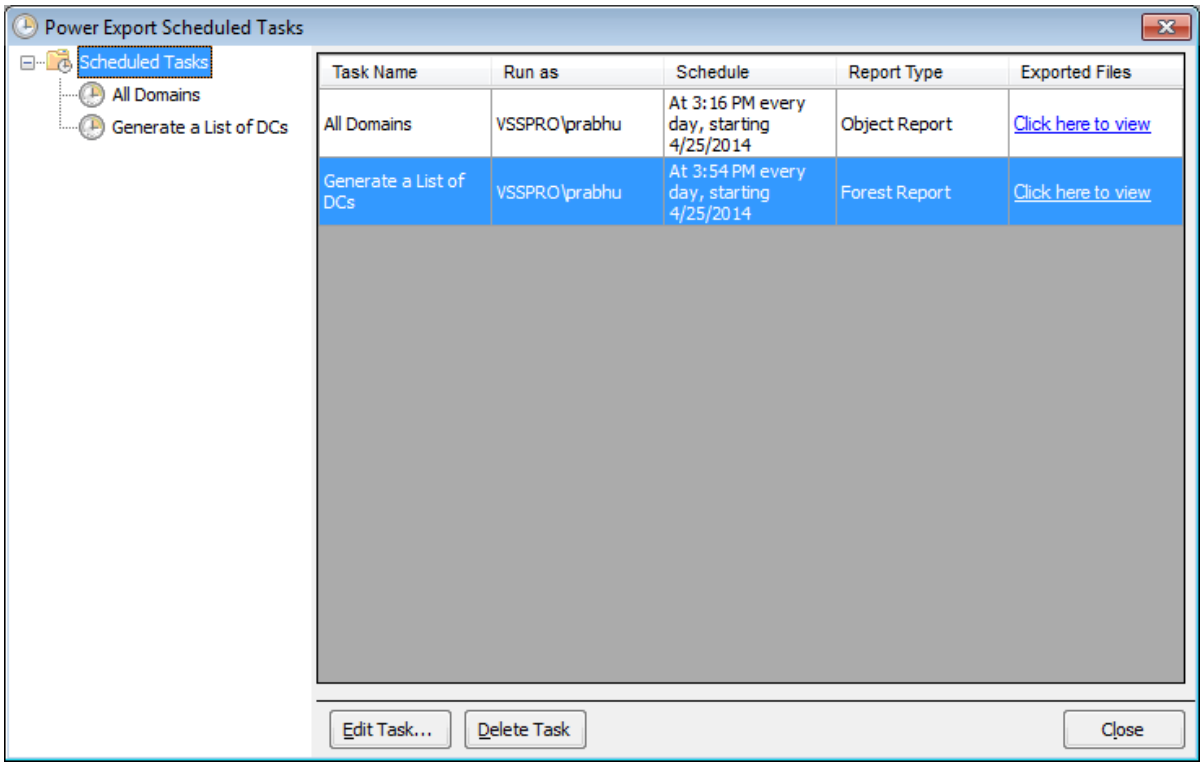
Step 5: Summary



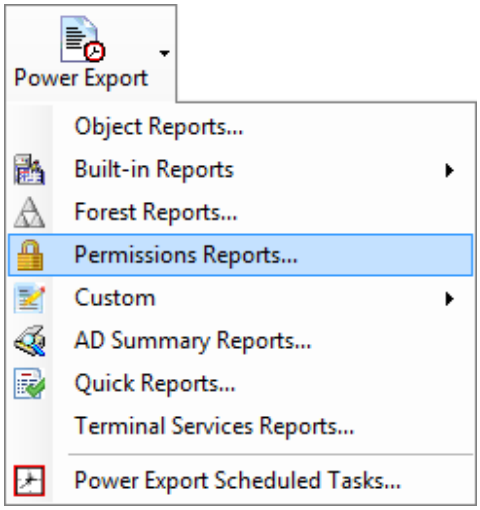
1) This step displays the ***summary*** *i*nformation of the task.

2) *Click* ***Finish*** to save the task details.

3) The task will be added to Windows ***Schedule Tasks*** and will be displayed in the ***Scheduled Tasks Manager*** Window as shown below:

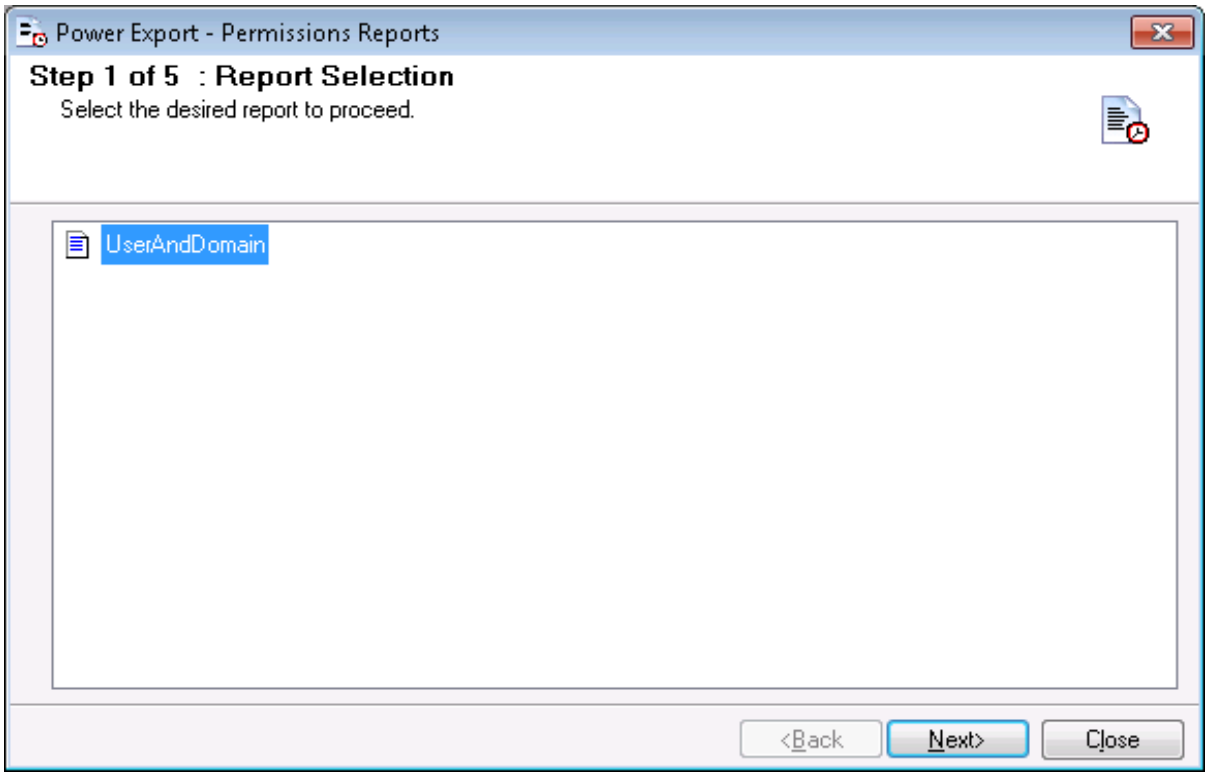


14.7 Schedule Permissions Reports



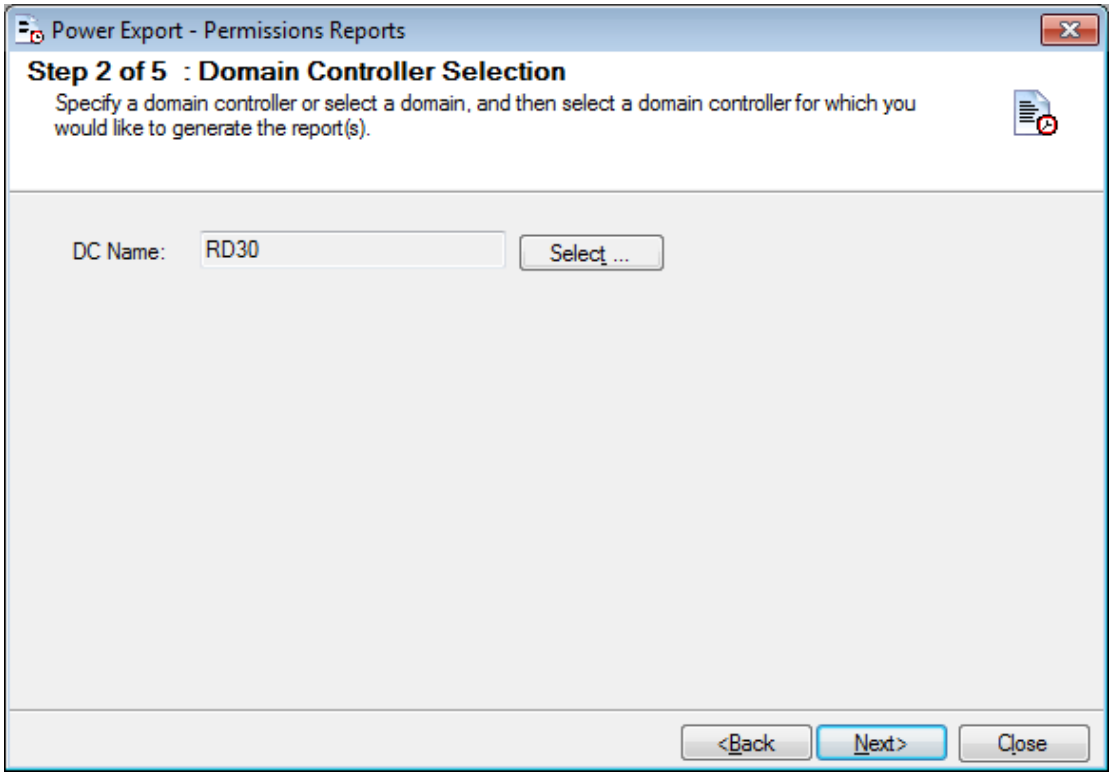
Select *option* under *Power Export*. This will bring up the ***Power Export*** *Wizard.*

Step 1: Report Selection


Power Export - Permissions Reports
Step 1 of 5 : Report Selection
Select the desired report to proceed.
UserAndDomain
<Back
Next>
Close

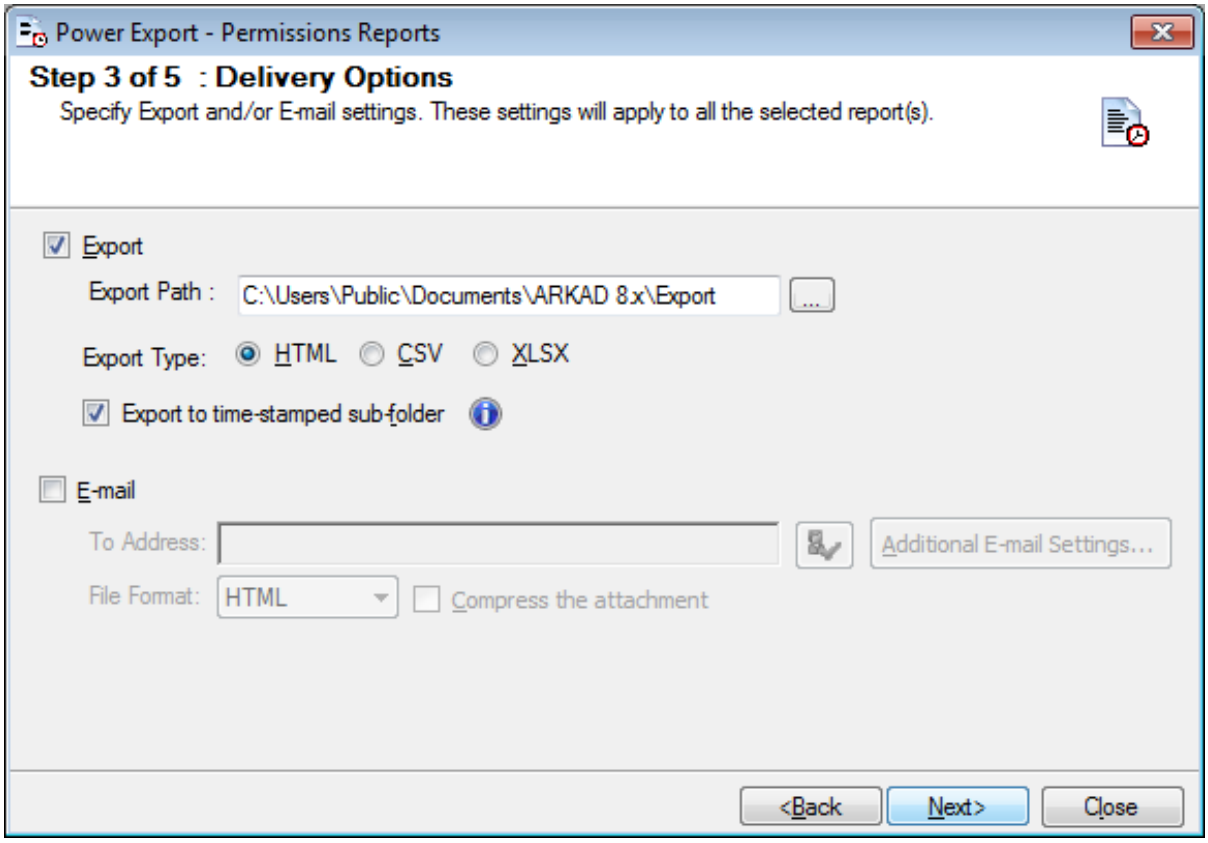
1) **Select the desired report. Only one report may be selected to run in a single task.**
2) *Click* ***Next*** to proceed to the *next* step. You may *Click Back* button anytime to come back to a previous step.

Step 2: Domain Controller Selection


Power Export - Permissions Reports
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) *Specify a domain controller for which you want to generate the selected custom report.* Click ***Select*** button to specify a domain controller. The Connection Manager will be displayed which will allow you to specify a domain controller.
2) *Click* ***Next*** to proceed to the *next* Step.

Step 3: Export/Email Options



1) *Change* the ***Export*** *or* ***Email*** settings as necessary.

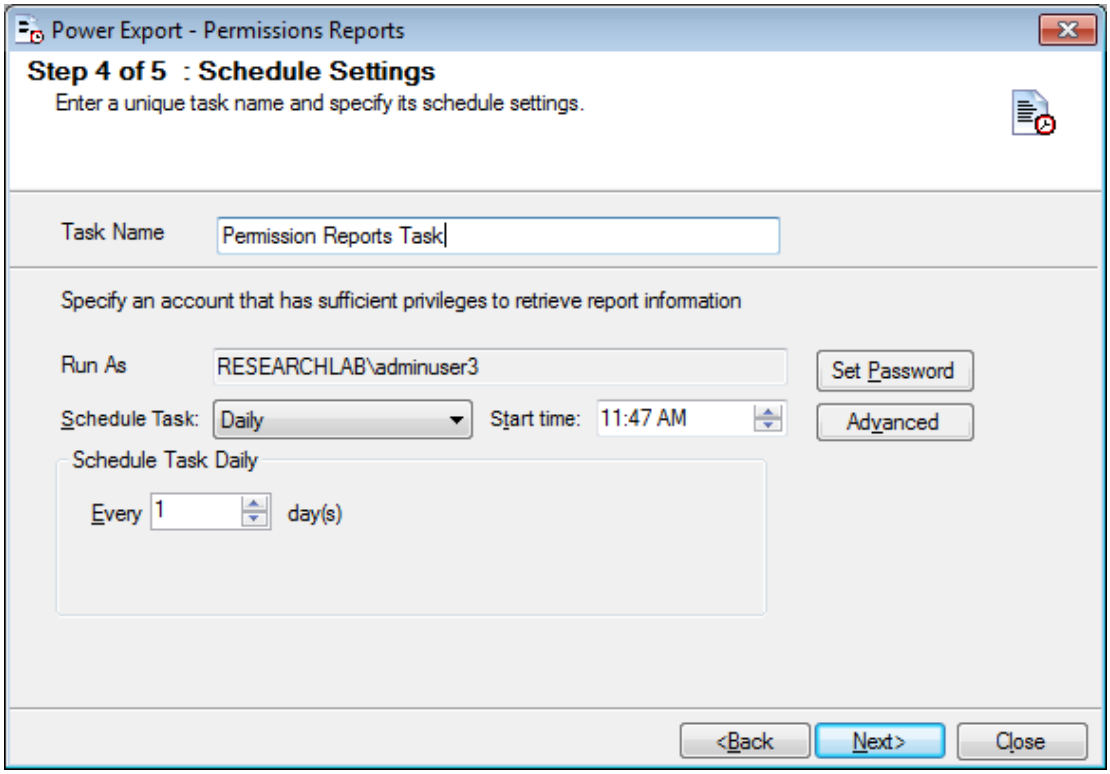
2) *Use* ***Browse*** button to *change* the ***export path***.

3) The ***export path*** refers to the *destination location* where the output file generated should be stored. By *default,* for each task, a *sub-folder* with the task name will be created under the specified export path. All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then *click* to clear ***"Export to time-stamped sub-folder"*** option.

NOTE: Clearing the "Export to time-stamped sub-folder" option will overwrite existing files, if any, in the specified export path.

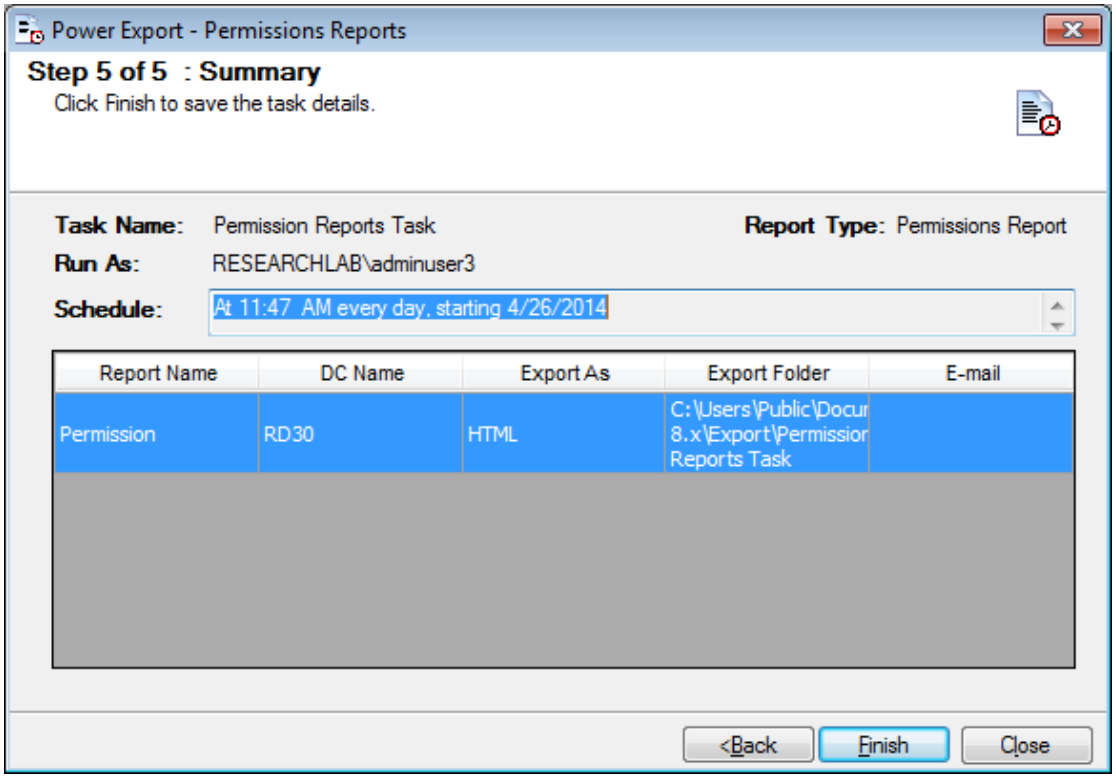
4) *Click* ***Next*** to proceed to *the next* step.

Step 4: Schedule Settings



1) Enter a ***unique name*** for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click* ***Next*** to proceed to the *next* and final step.

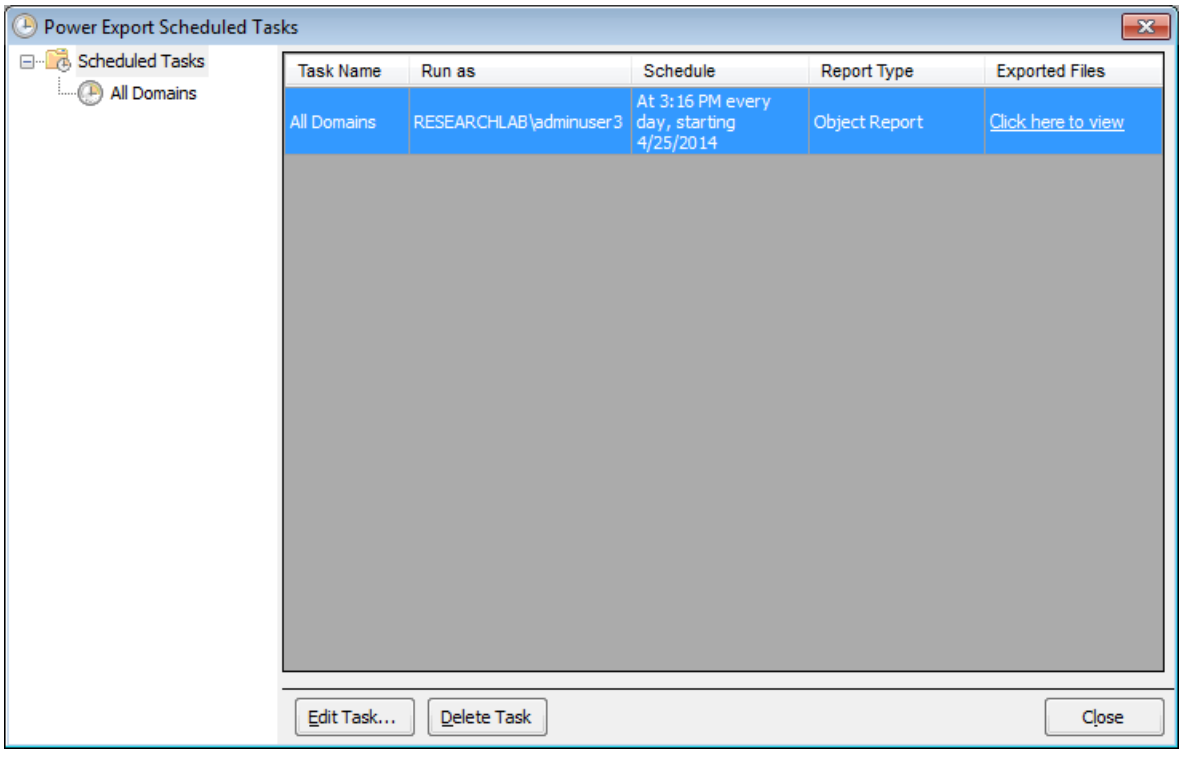
Step 5: Summary



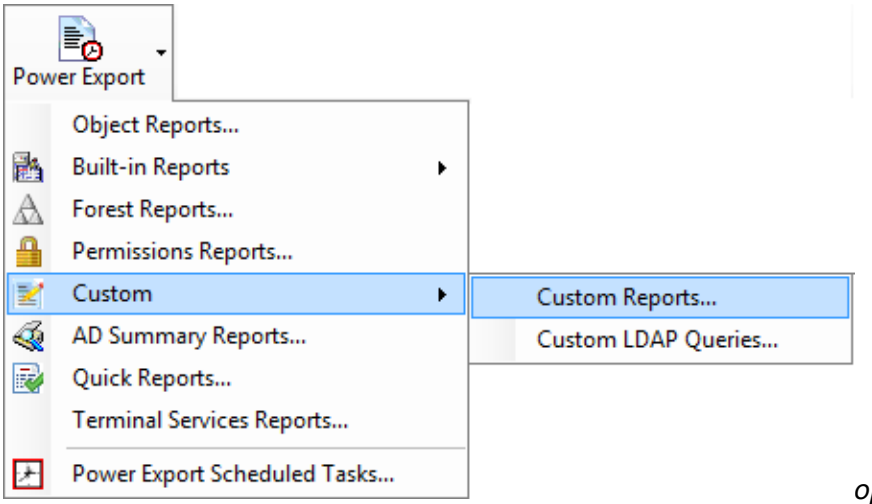
1) This step displays the ***summary*** information of the task.

2) *Click* ***Finish*** to save the ***task details.***

3) The task will be added to Windows *Schedule Tasks* and will be displayed in the ***Scheduled Tasks Manager*** Window as shown below:

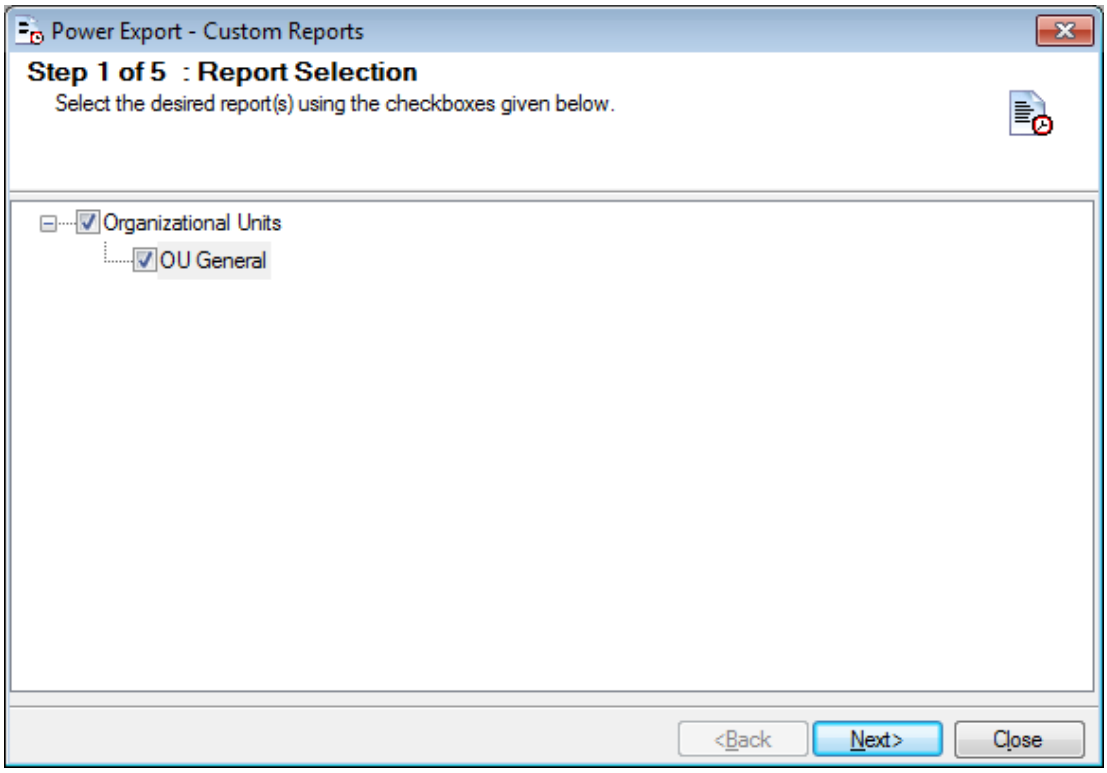


14.8 Schedule Custom Reports



Select *option* under *Power Export.* This will bring up the ***Power Export*** *Wizard.*

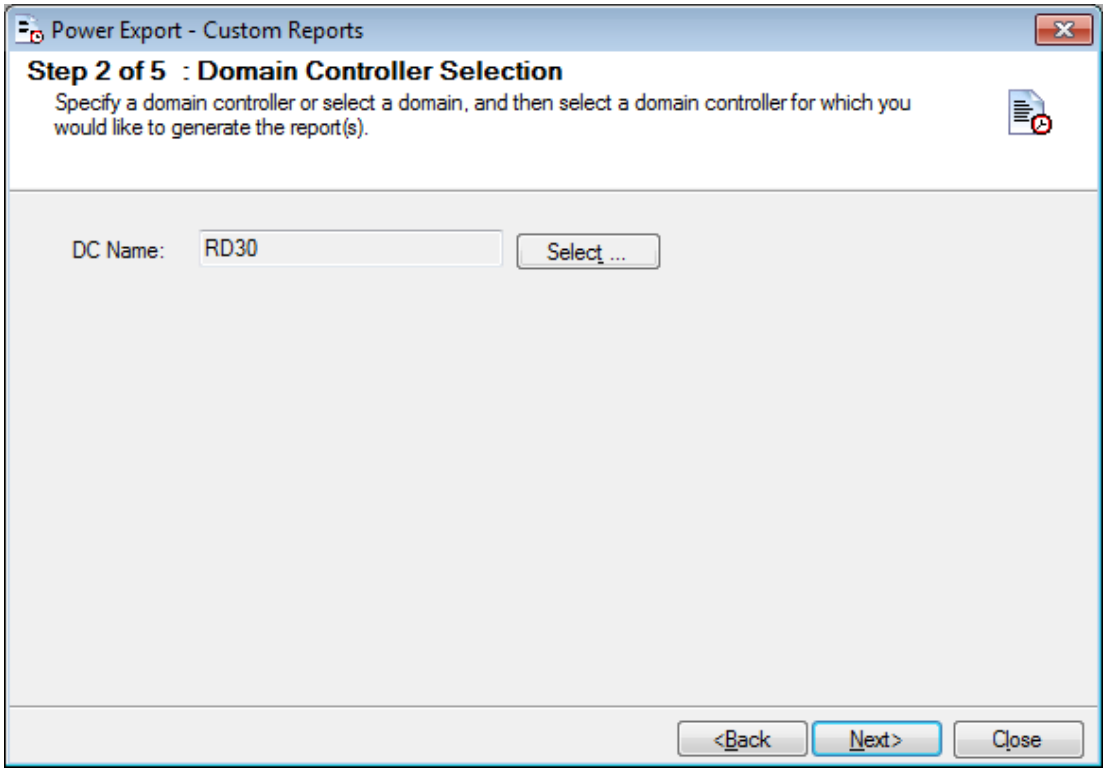
Step 1: Report Selection


Power Export - Custom Reports
Step 1 of 5 : Report Selection
Select the desired report(s) using the checkboxes given below.
Organizational Units
OU General
<Back
Next>
Close

`

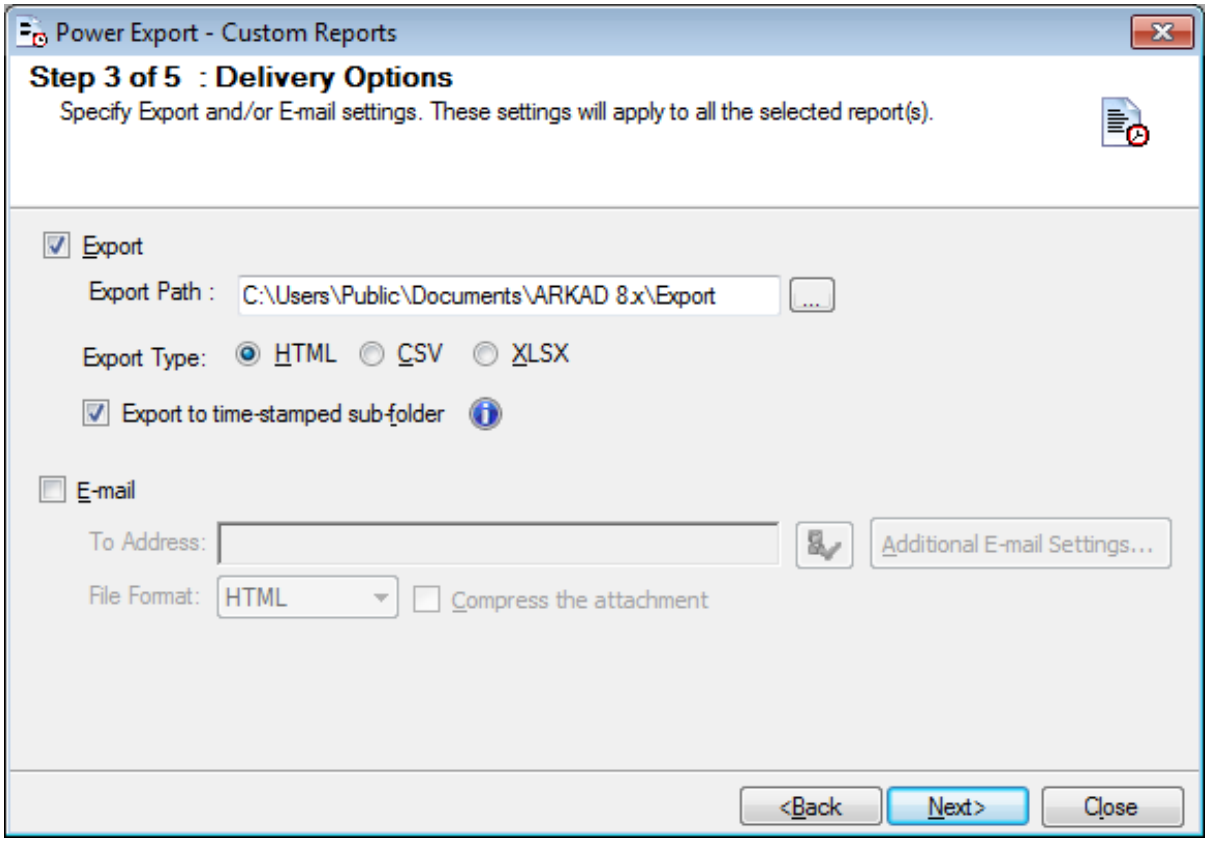
1) ***Select*** the report(s) using the ***checkboxes*** to the left of the reports. You may select any number of reports to run in a single task.
2) *Click* ***Next*** to proceed to the *next* step. You may *Click Back* button anytime to come back to a previous step.

Step 2: Domain Controller Selection


Power Export - Custom Reports
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) ***Specify a domain controller for which you want to generate the selected custom report.*** Click ***Select*** *button* to specify a domain controller. The Connection Manager will be displayed which will allow you to specify a domain controller.
2) *Click* ***Next*** to proceed to the next Step.

Step 3: Export/Email Options

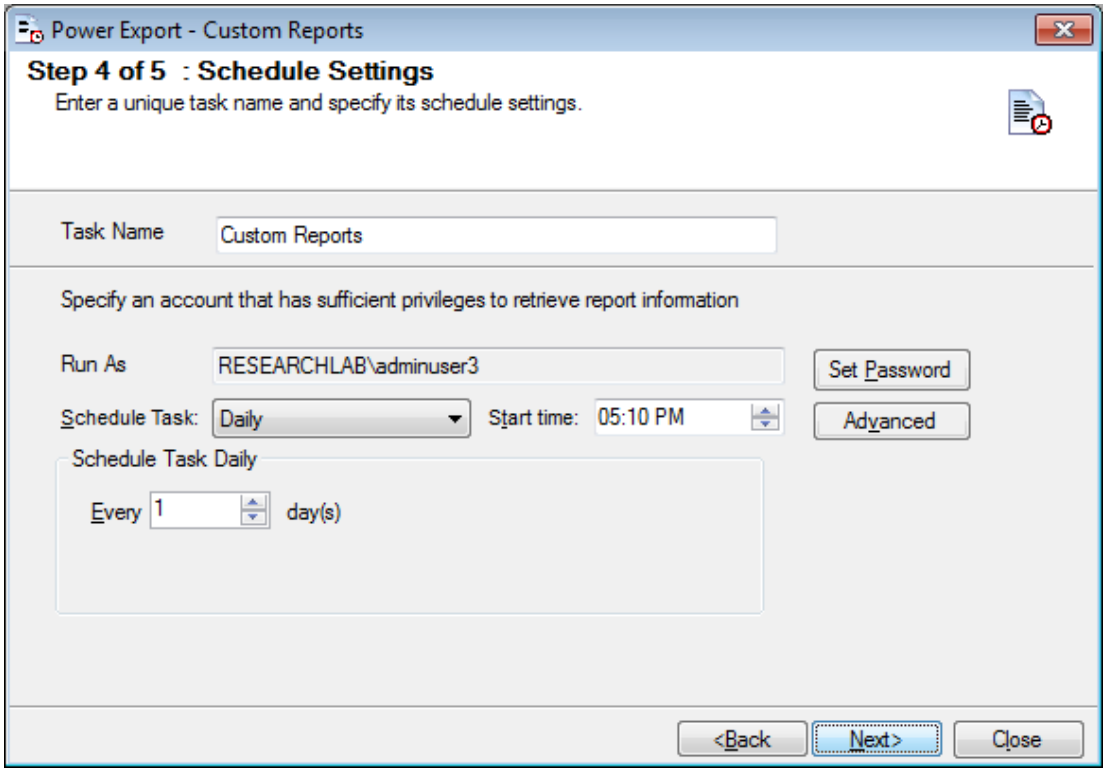


1) *Change* the ***Export*** *or* ***Email*** settings as necessary.
2) *Use* ***Browse*** *button* to *change* the **export path.**
3) The ***export path*** refers to the *destination location* where the output file generated should be stored. By *default*, for each task, a *sub-folder* with the task name will be created under the specified export path. All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear ***"Export to time-stamped sub-folder"*** option.

   NOTE: Clearing the "Export to time-stamped sub-folder" option will *overwrite* existing files, if any, in the specified export path.

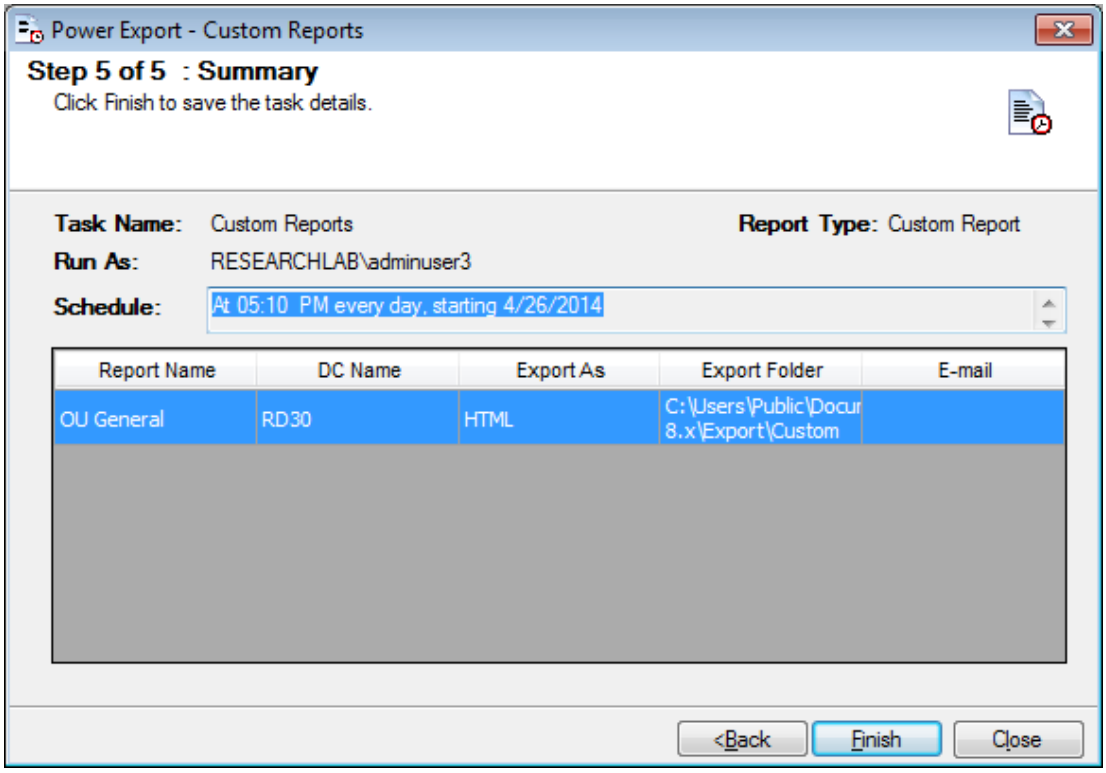
4) *Click* ***Next*** to Proceed to the *Next* Step.

Step 4: Schedule Settings



1) *Enter* a ***unique name*** for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click* ***Next*** to proceed to the next and final step.

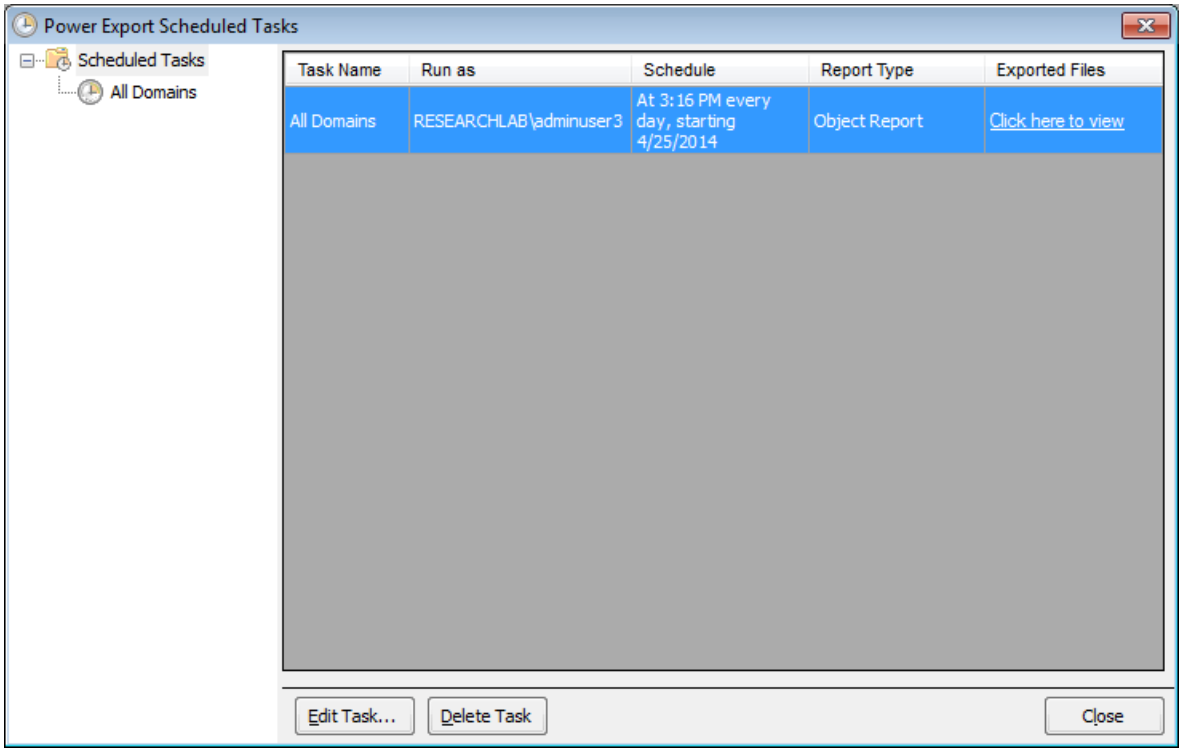
Step 5: Summary



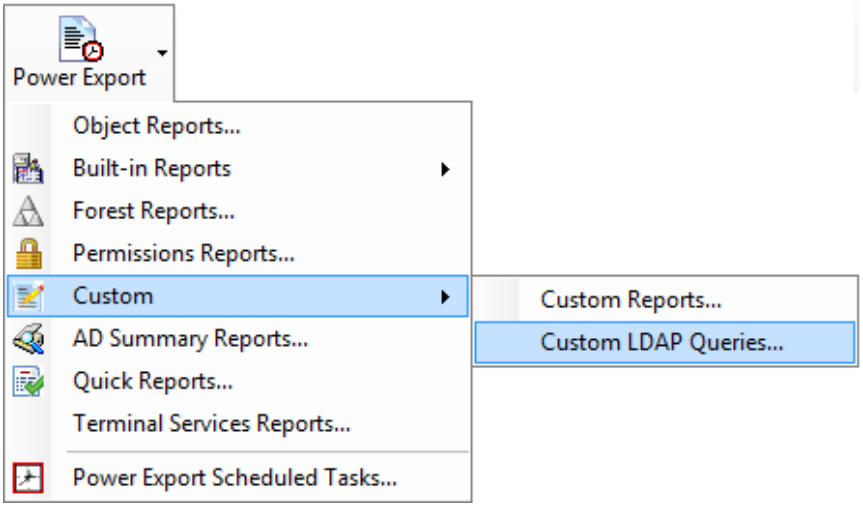
1) This step displays the ***summary*** *information* of the task.

2) *Click* ***Finish*** to save the ***task details***.

3) The task will be added to Windows Schedule Tasks and will be displayed in the ***Scheduled Tasks Manager*** Window as shown below:

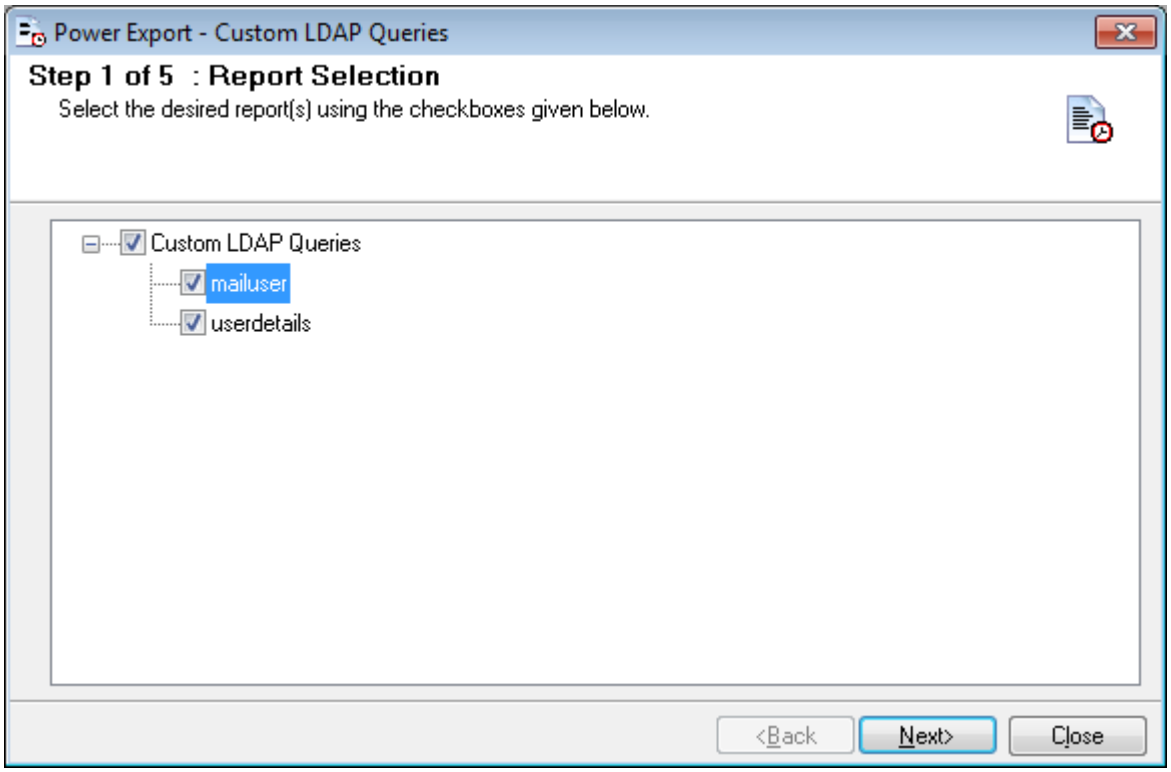


14.9 Schedule Custom LDAP Queries Reports



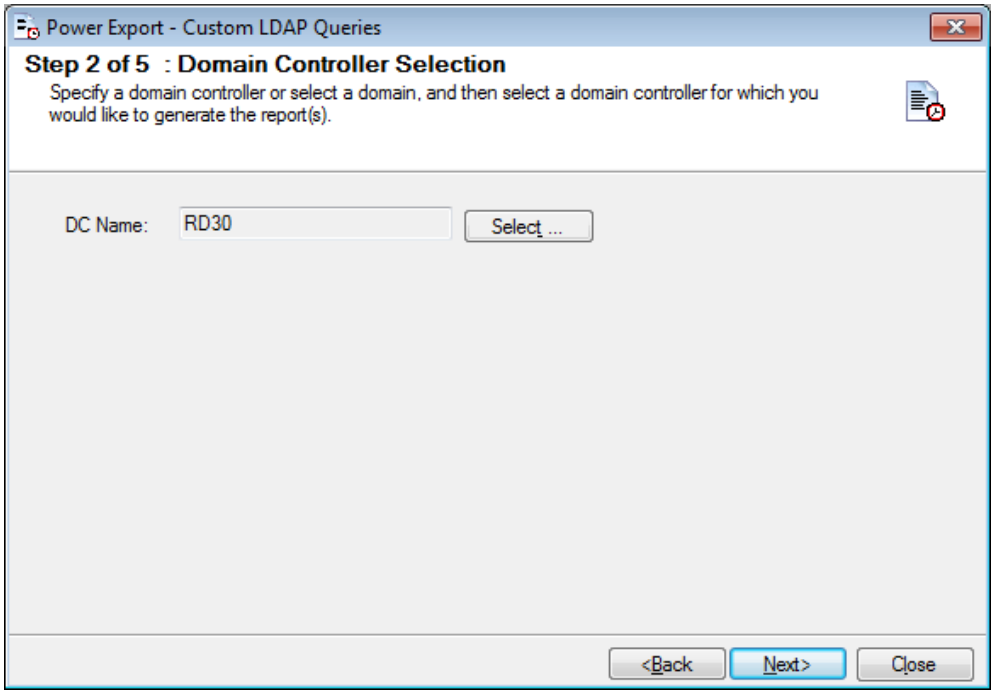
Select *option* under *Power Export.* This will bring up the ***Power Export*** *Wizard.*

Step 1: Report Selection


Power Export - Custom LDAP Queries
Step 1 of 5 : Report Selection
Select the desired report(s) using the checkboxes given below.
Custom LDAP Queries
mailuser
userdetails
<Back
Next>
Close

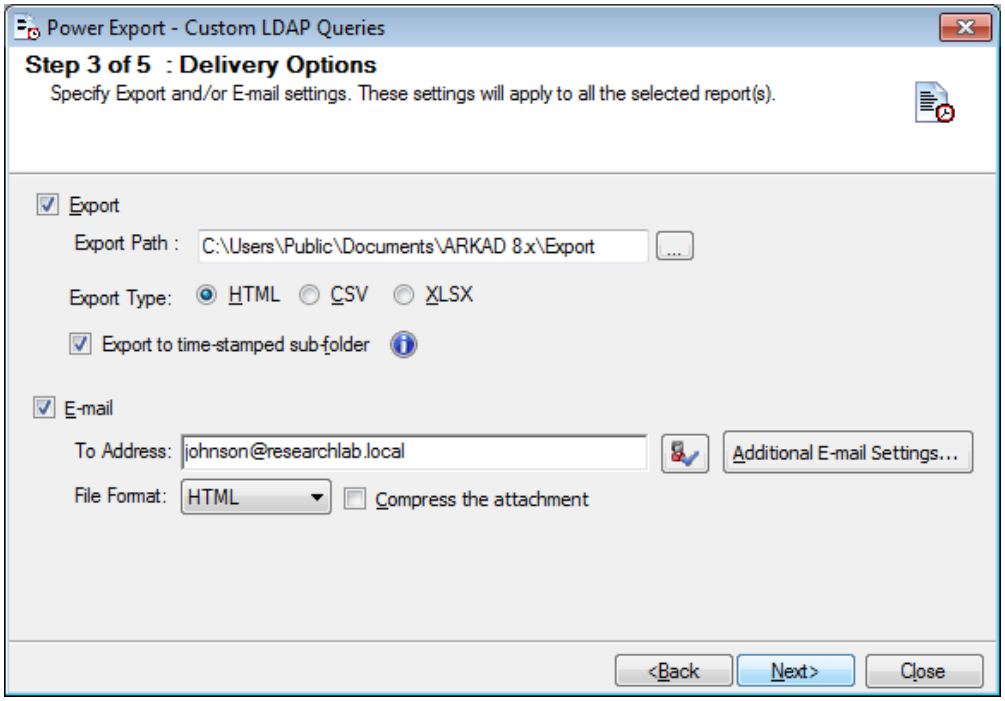
1) ***Select*** the report(s) using the ***checkboxes*** to the left of the reports. You may select any number of reports to run in a single task.
2) *Click* ***Next*** to proceed to the next step. You may *Click Back* button anytime to come back to a previous step.

Step 2: Domain Controller Selection


Power Export - Custom LDAP Queries
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) Specify a ***domain controller*** for which you want to *generate* the selected ***Custom LDAP Query report***. Click ***Select*** button to specify a domain controller. The *Connection Manager* will be displayed which will allow you to specify a domain controller
2) Click ***Next*** to proceed to the next Step

Step 3: Export/Email Options



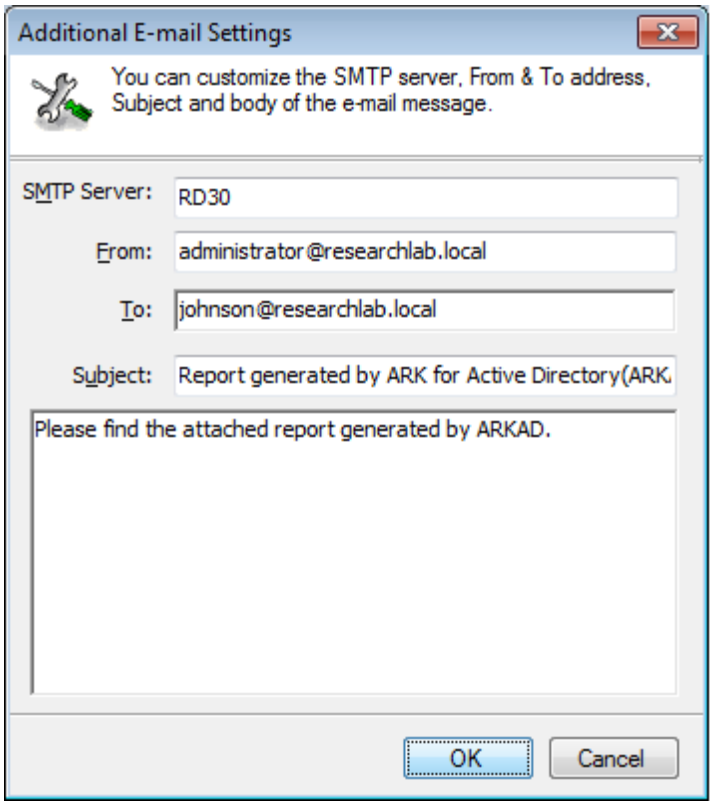
1) *Change* the ***Export or Email*** settings as necessary.

2) *Use* ***Browse*** *button* to change the ***export path.***

3) The ***export path*** refers to the *destination location* where the output file generated should be stored. By *default,* for each task, a *sub-folder* with the task name will be created under the specified export path. All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-dd hh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear ***"Export to time-stamped sub-folder"*** option.

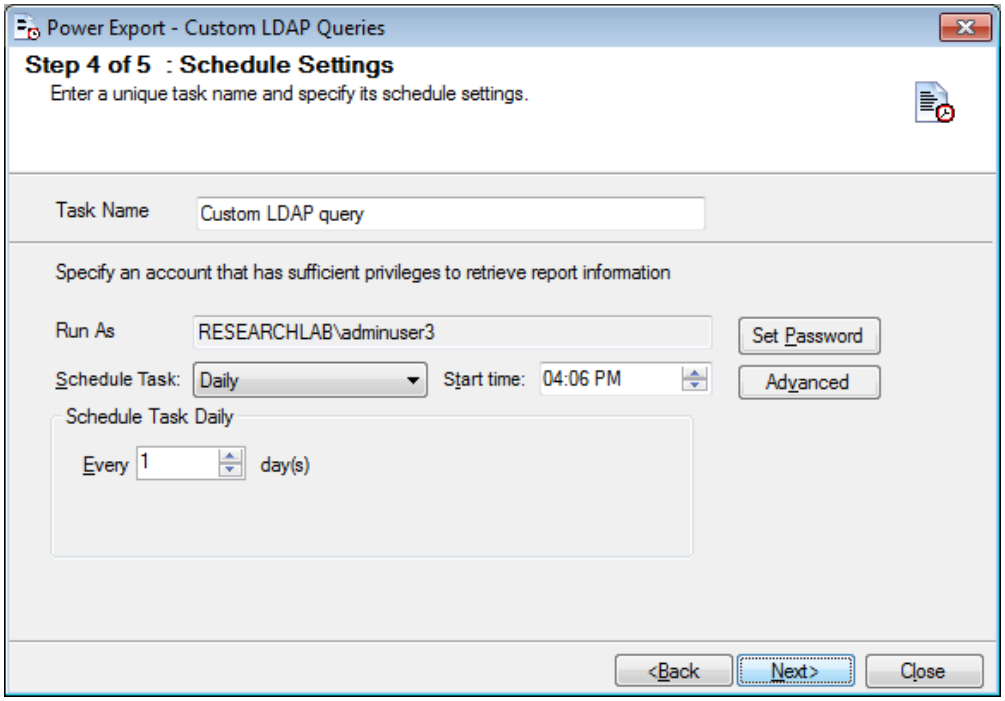
NOTE: Clearing the "Export to time-stamped sub-folder" option will *overwrite* existing files, if any, in the specified export path.

4) *Click* ***Additional E-mail Settings*** button to specify optional e-mail settings as shown below.



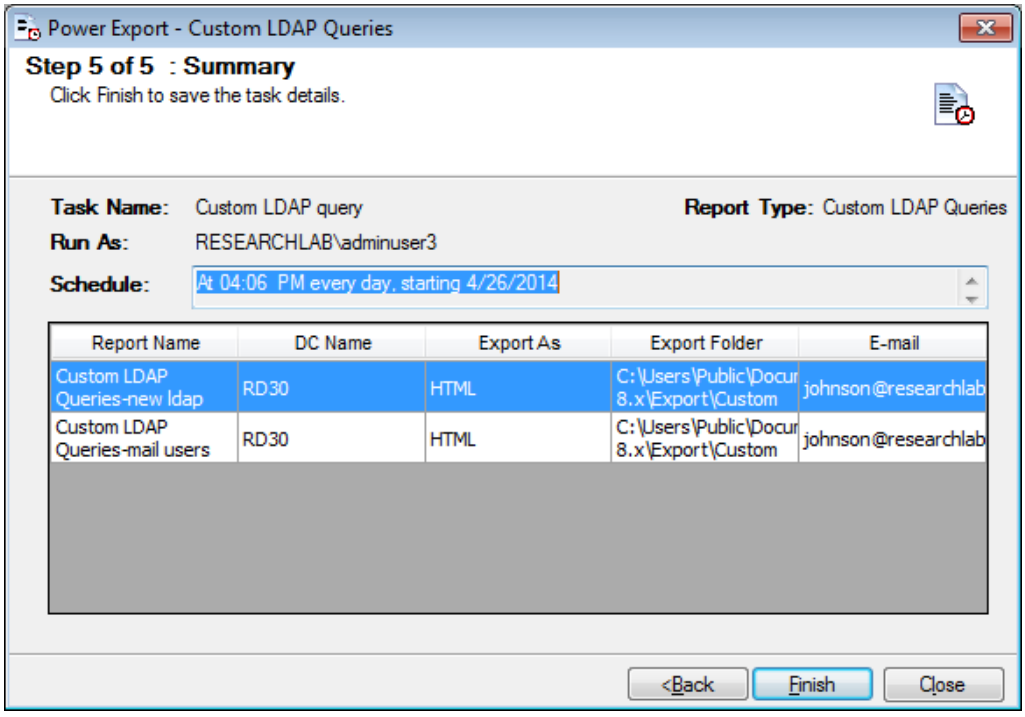
5) *Click* ***Next*** to Proceed to the *Next* Step.

Step 4: Schedule Settings



1) *Enter* a ***unique name*** for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click* ***Next*** to proceed to the next and final step.

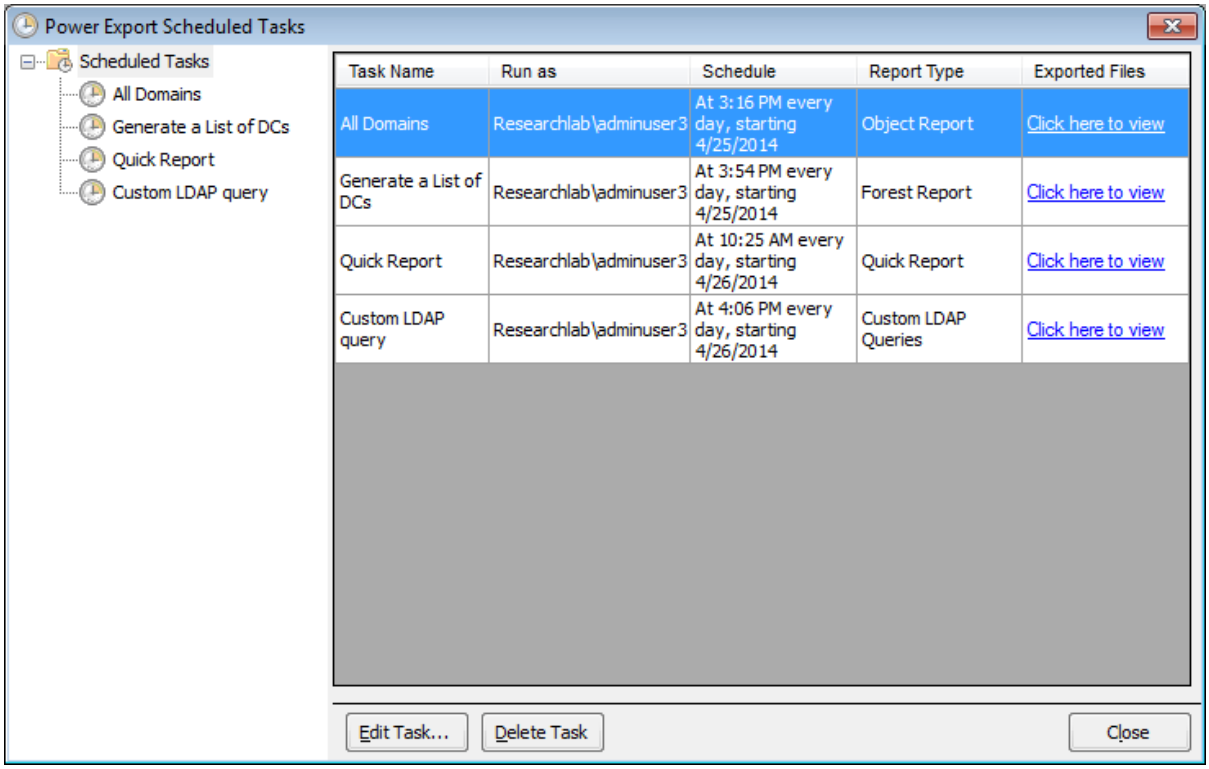
Step 5: Summary



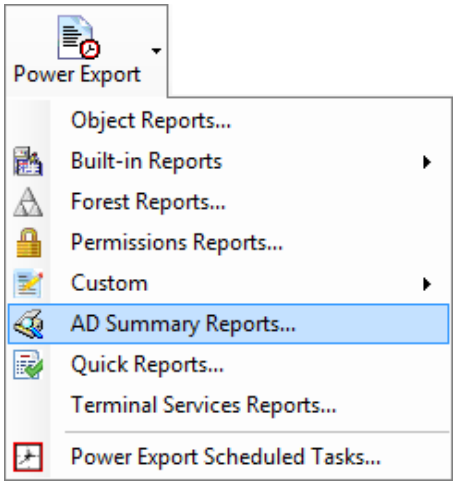
1) This step displays the ***summary*** information of the task.

2) *Click* ***Finish*** to save *the* ***task details***.

3) The task will be added to Windows Schedule Tasks and will be displayed in the ***Scheduled Tasks Manager*** Window as shown below:

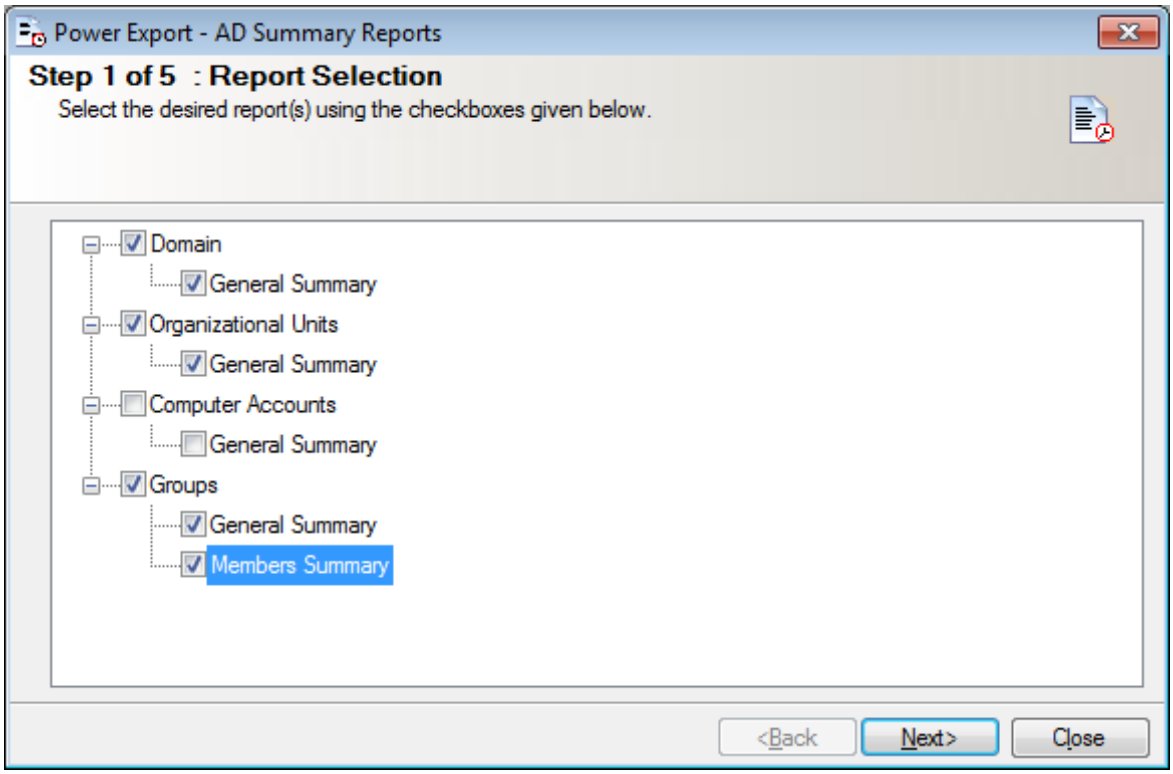


14.10 Schedule AD Summary Reports



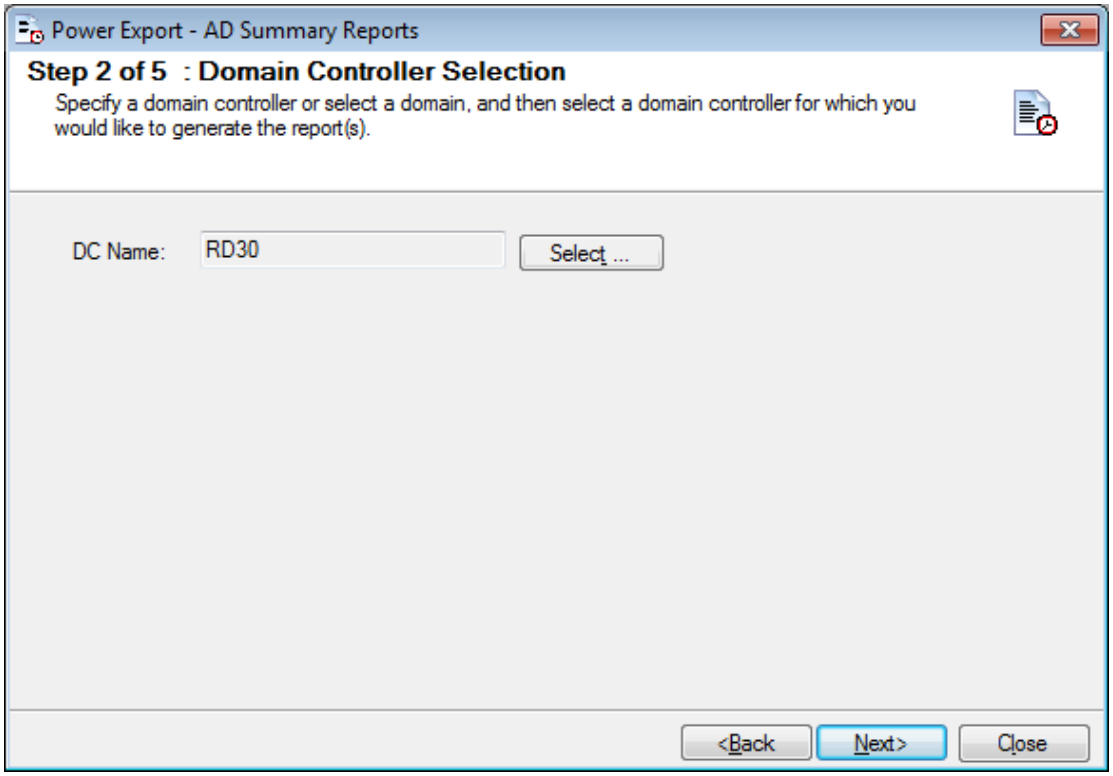
Select *option* under *Power Export.* This will bring up the ***Power Export*** *Wizard.*

Step 1: Report Selection



1) ***Select*** the report(s) using the ***checkboxes*** to the left of the reports. You may select any number of reports to run in a single task.
2) *Click* ***Next*** to proceed to the next step. You may Click *Back* button anytime to come back to a previous step.

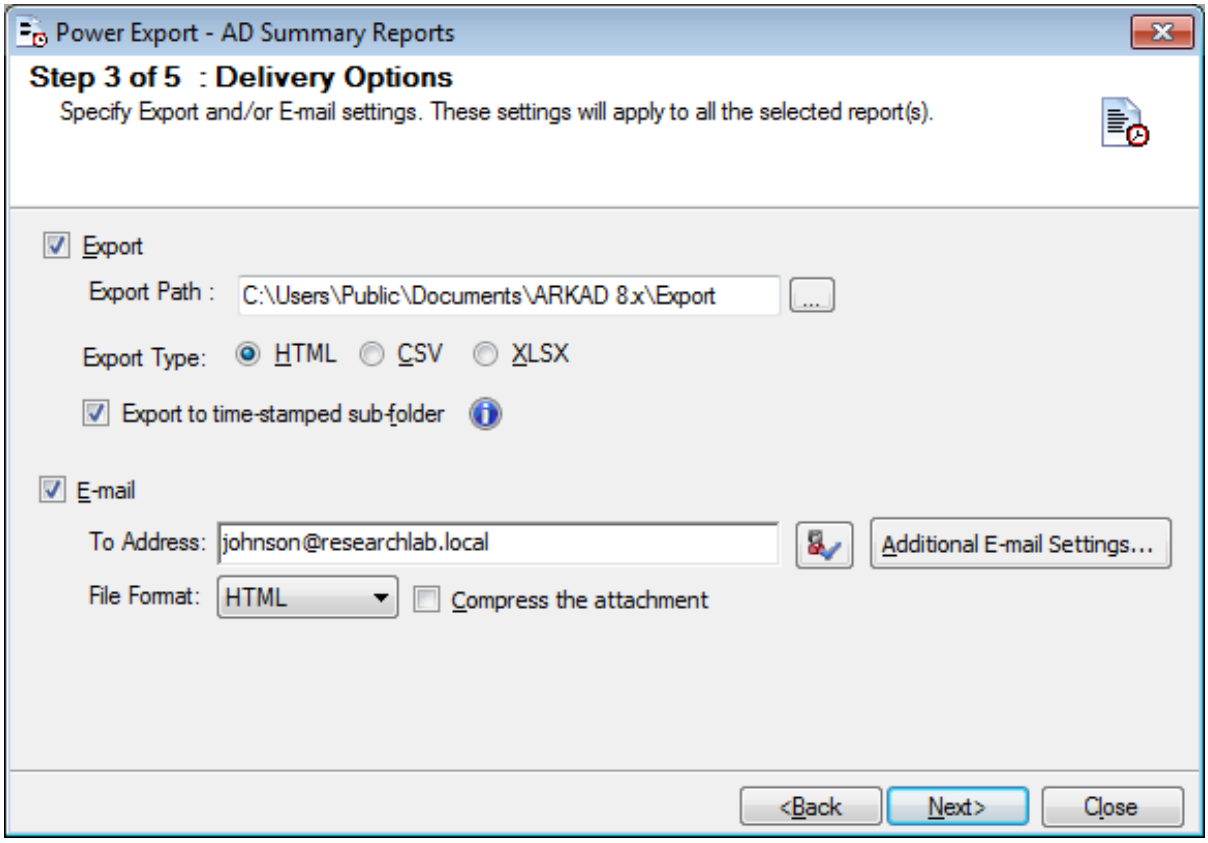
Step 2: Domain Controller Selection


Power Export - AD Summary Reports
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) Specify a domain controller for which you want to generate the selected custom report. Click Select button to specify a ***domain controller***. The ***Connection Manager*** will be displayed which will allow you to specify a domain controller

2) *Click* ***Next*** to proceed to the *next* Step.

Step 3: Export/Email Options



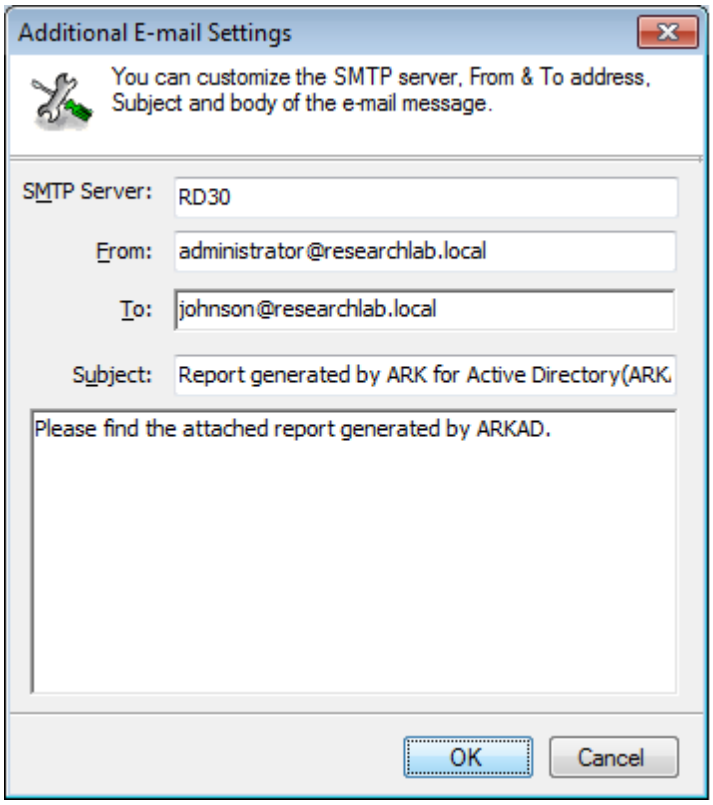
1) *Change* the ***Export*** *or* ***Email*** settings as necessary.

2) *Use* ***Browse*** *button* to *change the* ***export path.***

3) The *export path* refers to the *destination location* where the output file generated should be stored. By *default*, for each task, a *sub-folder* with the task name will be created under the specified export path. All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear ***"Export to time-stamped sub-folder"*** option.

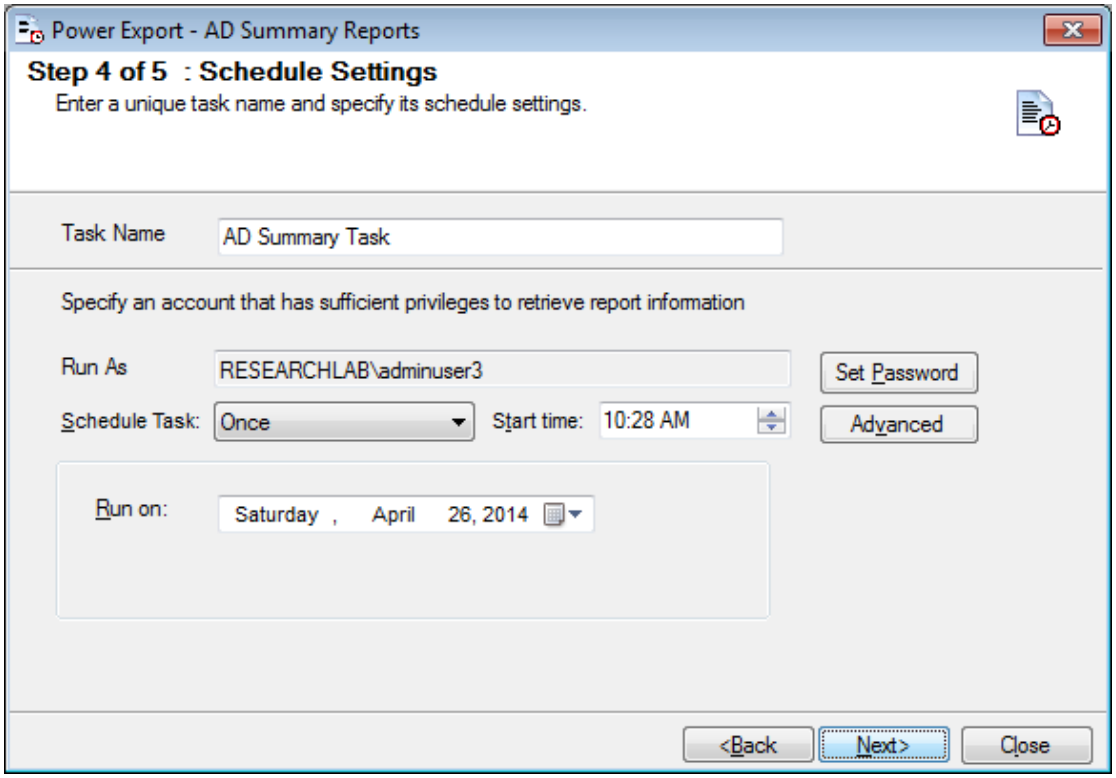
NOTE: Clearing the "Export to time-stamped sub-folder" option will *overwrite* existing files, if any, in the specified export path.

4) *Click* ***Additional E-mail Settings*** button to specify optional e-mail settings as shown below.



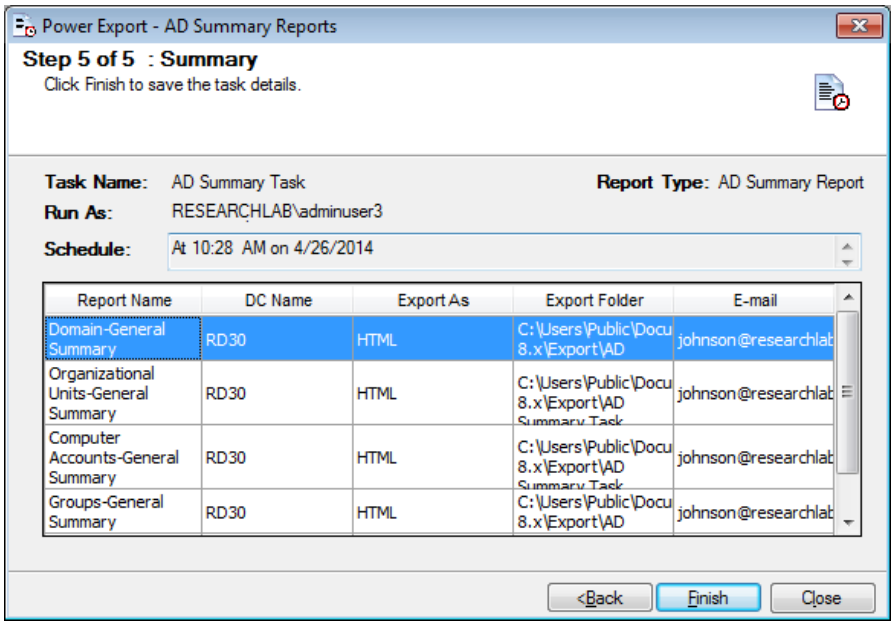
5) *Click* ***Next*** to proceed to the next step.

Step 4: Schedule Settings



1) *Enter a **unique name*** for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click **Next*** to proceed to the next and final step.

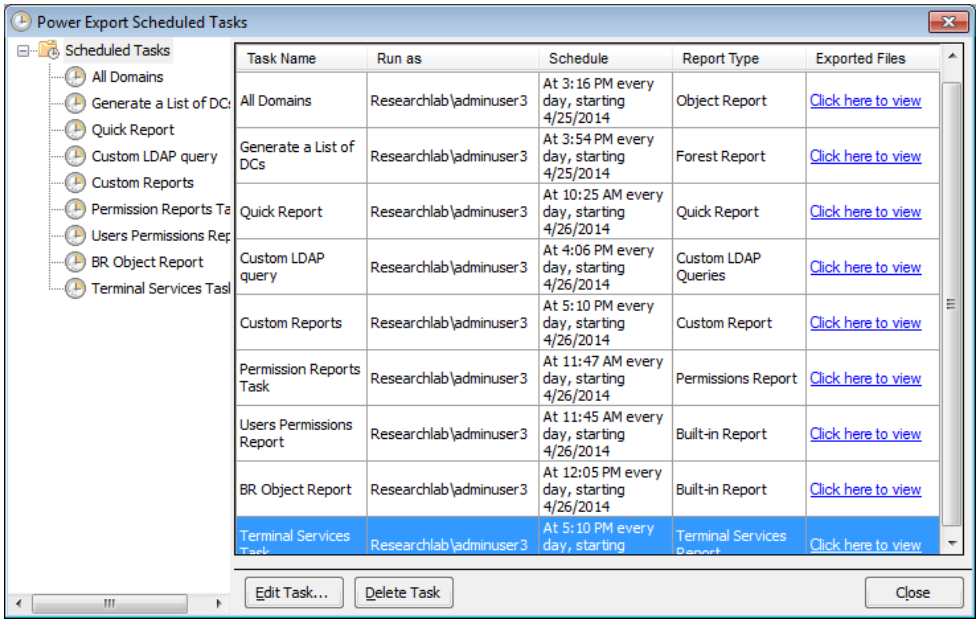
Step 5: Summary



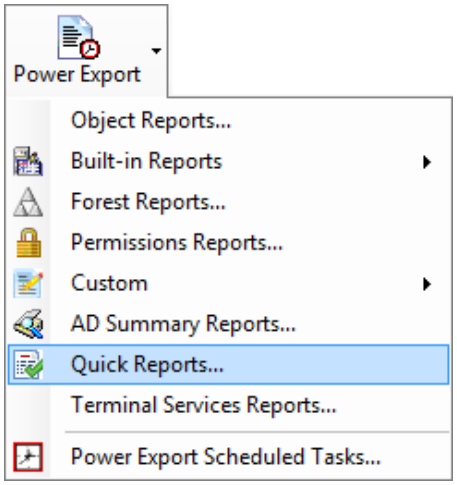
1) This step displays the ***summary*** information of the task.

2) *Click* ***Finish*** to save the task details.

3) The task will be added to Windows ***Schedule Tasks*** and will be displayed in the ***Scheduled Tasks Manager*** Window as shown below:

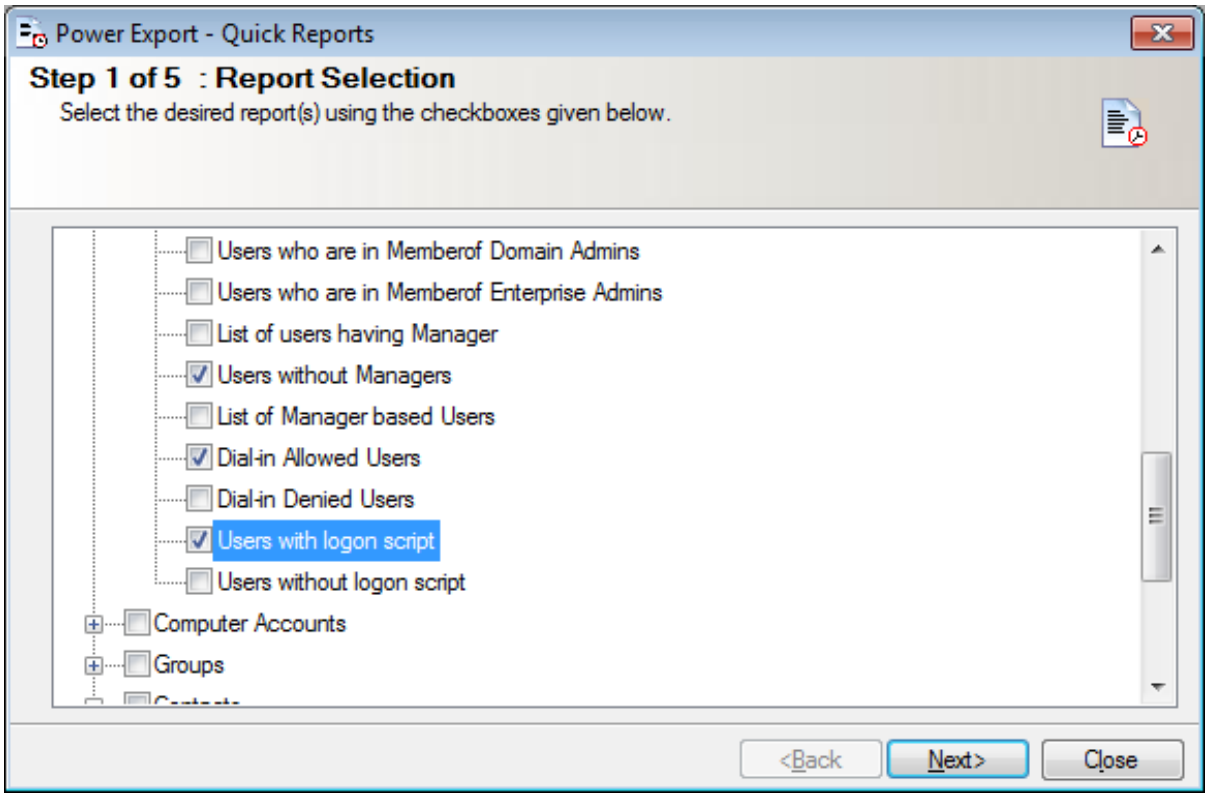


14.11 Schedule Quick Reports



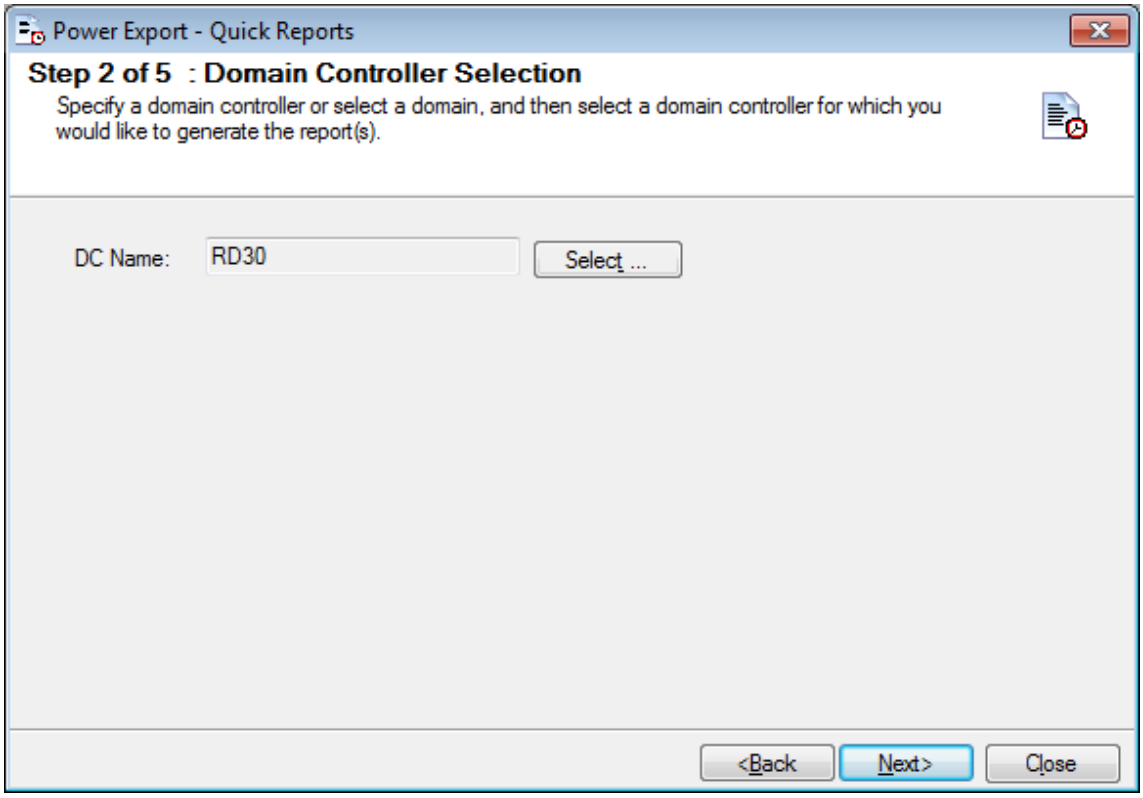
Select *option* under *Power Export.* This will bring up the ***Power Export*** *Wizard.*

Step 1: Report Selection


Power Export - Quick Reports
Step 1 of 5 : Report Selection
Select the desired report(s) using the checkboxes given below.
Users who are in Memberof Domain Admins
Users who are in Memberof Enterprise Admins
List of users having Manager
Users without Managers
List of Manager based Users
Dial-in Allowed Users
Dial-in Denied Users
Users with logon script
Users without logon script
Computer Accounts
Groups
<Back
Next>
Close

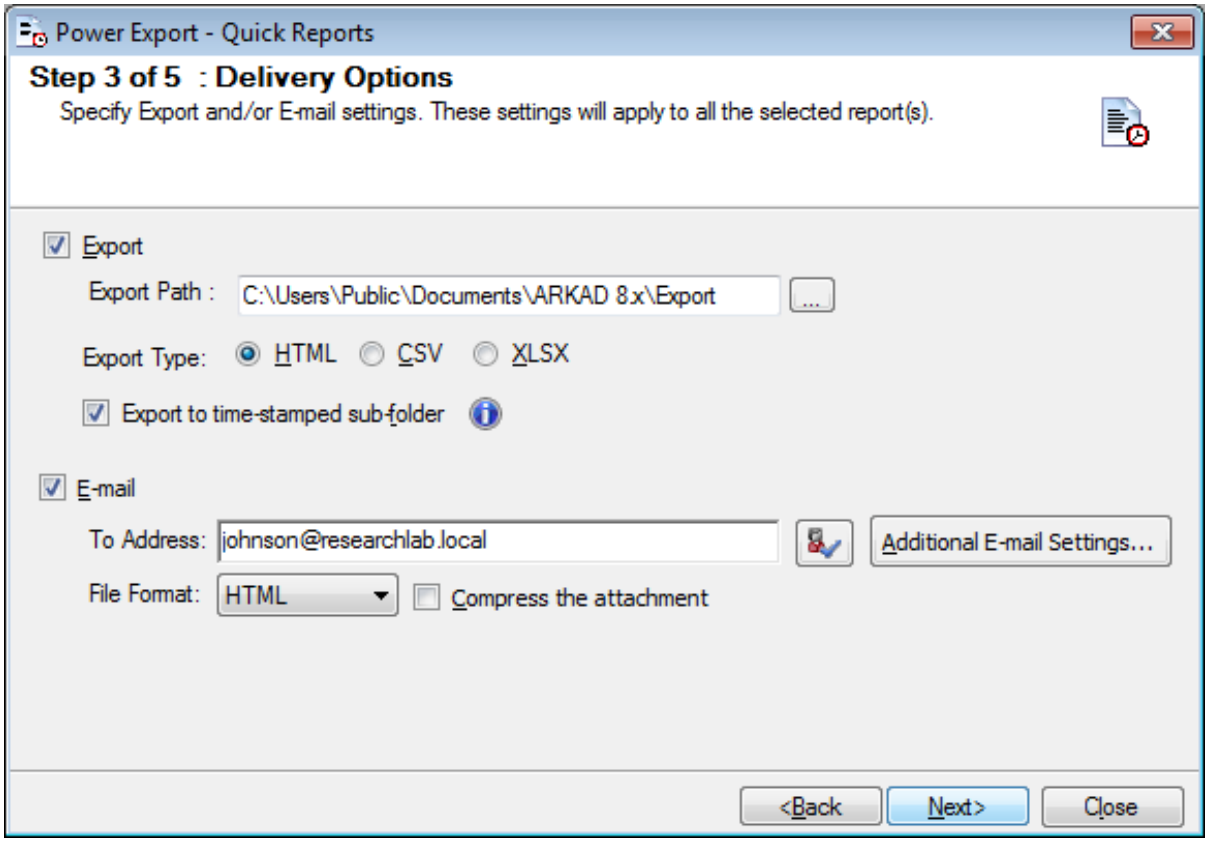
1) ***Select*** the report(s) using the ***checkboxes*** to the left of the reports. You may select any number of reports to run in a single task.
2) *Click* ***Next*** to proceed to the next step. You may Click *Back* button anytime to come back to a previous step.

Step 2: Domain Controller Selection


Power Export - Quick Reports
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) Specify a domain controller for which you want to generate the selected custom report. Click ***Select*** *button* to specify a ***domain controller***. The ***Connection Manager*** will be displayed which will allow you to specify a domain controller
2) *Click* ***Next*** to proceed to the next Step.

Step 3: Export/Email Options



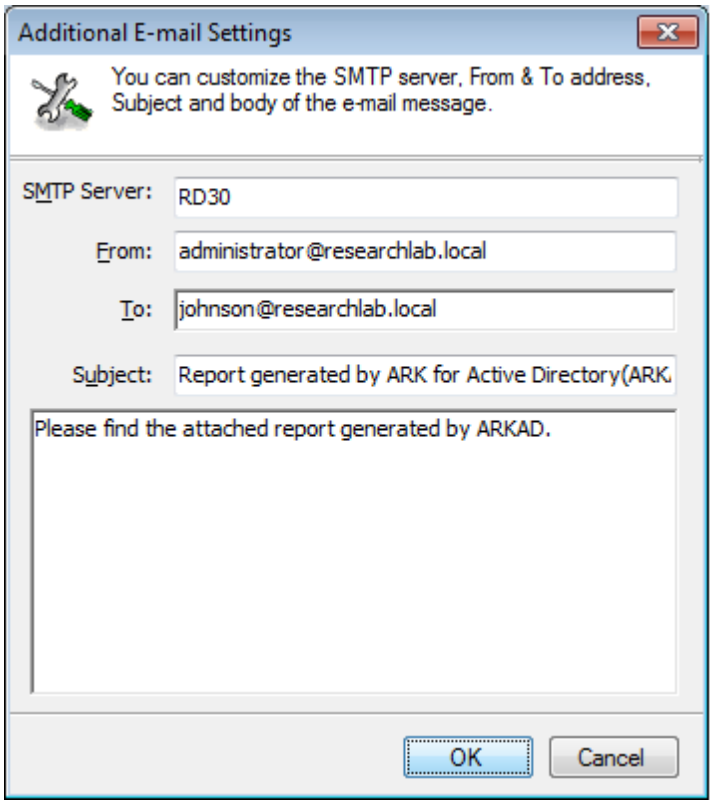
1) *Change* the ***Export*** *or* ***Email*** settings as necessary.

2) *Use* ***Browse*** *button* to change the ***export path.***

3) The ***export path*** refers to the *destination location* where the output file generated should be stored. By *default*, for each task, a *sub-folder* with the task name will be created under the specified export path. All selected reports will be exported to a *time-stamped folder*, in the format "yyyy-mm-ddhh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear ***"Export to time-stamped sub-folder"*** option.

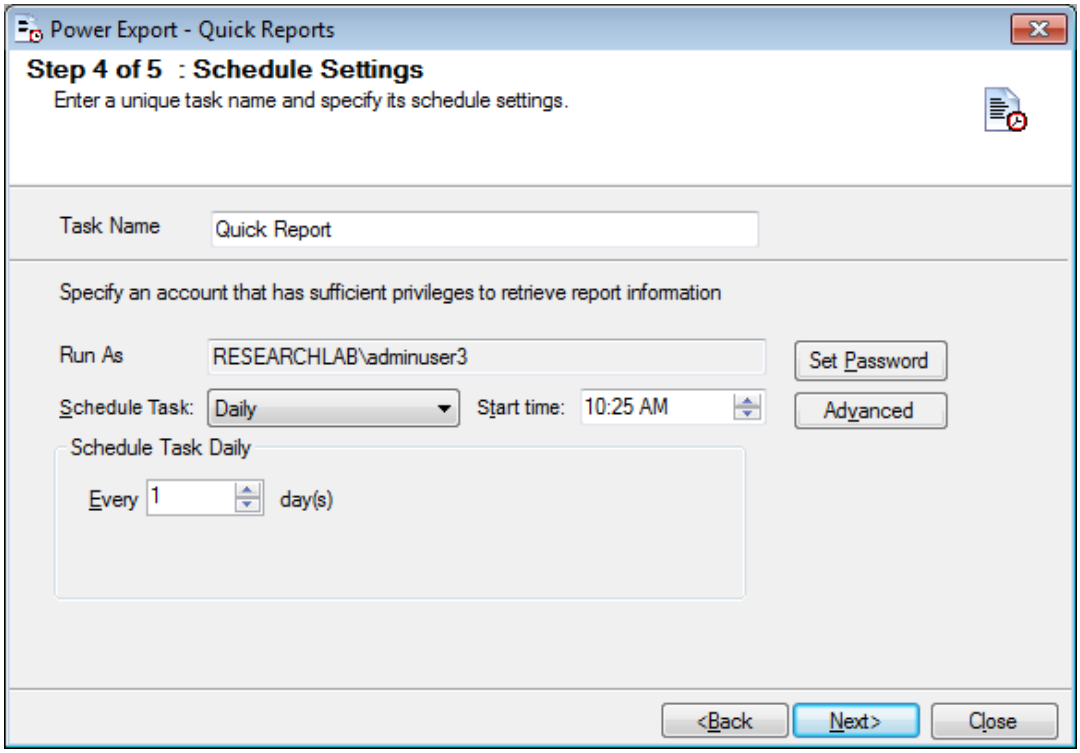
NOTE: Clearing the "Export to time-stamped sub-folder" option will *overwrite* existing files, if any, in the specified export path.

4) *Click* ***Additional E-mail Settings*** button to specify optional e-mail settings as shown below.



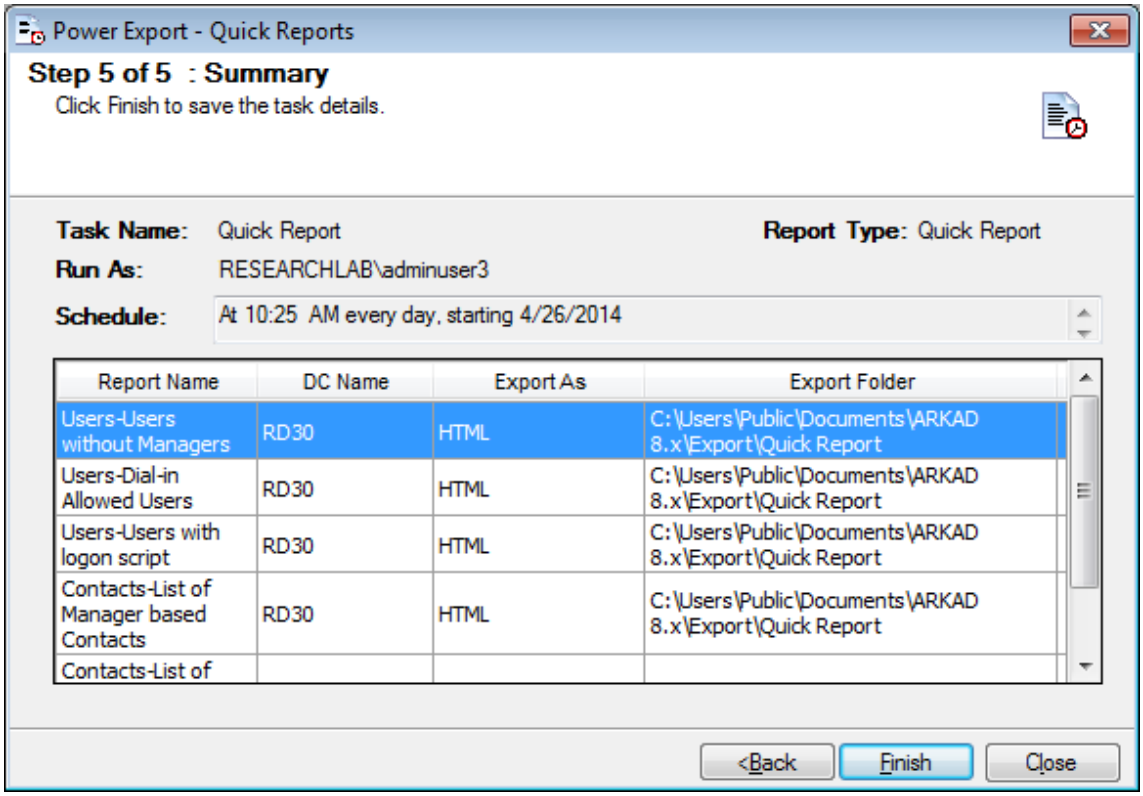
5) *Click* ***Next*** to proceed to the *next* step.

Step 4: Schedule Settings



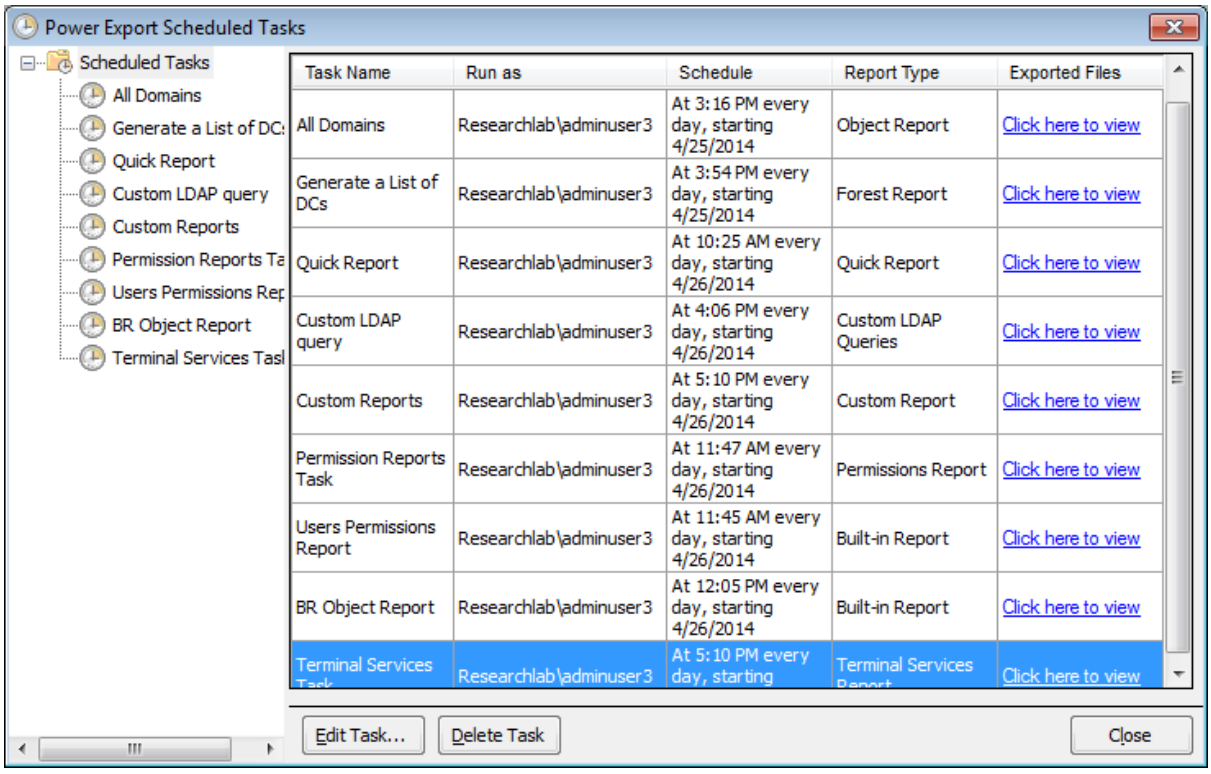
1) *Enter* a ***unique name*** for the task.
2) The task will run on currently logged on user and ***set password*** for the currently logged on user.
3) *Change* the ***task schedule*** settings as required.
4) *Click* ***Next*** to proceed to the next and final step.

Step 5: Summary

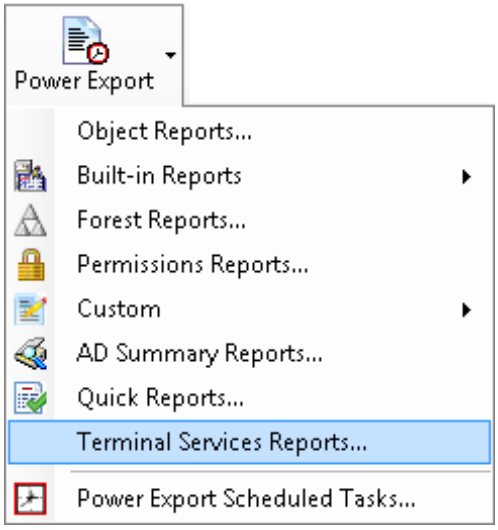


1) This step displays the ***summary*** information of the task.
2) *Click* ***Finish*** to save the task details.

3) The task will be added to **Windows Schedule Tasks** and will be displayed in the **Scheduled Tasks Manager** Window as shown below:

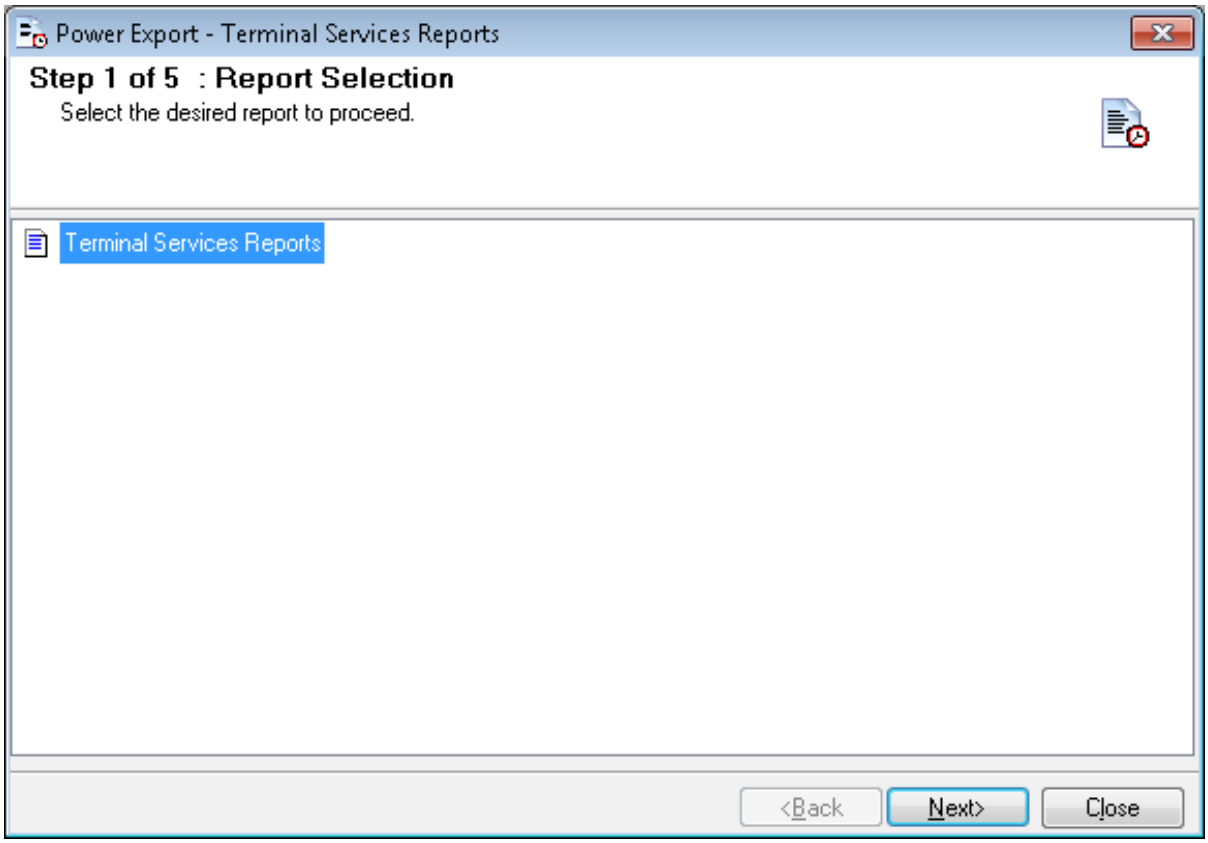


14.12 Schedule Terminal Services Reports

Select 

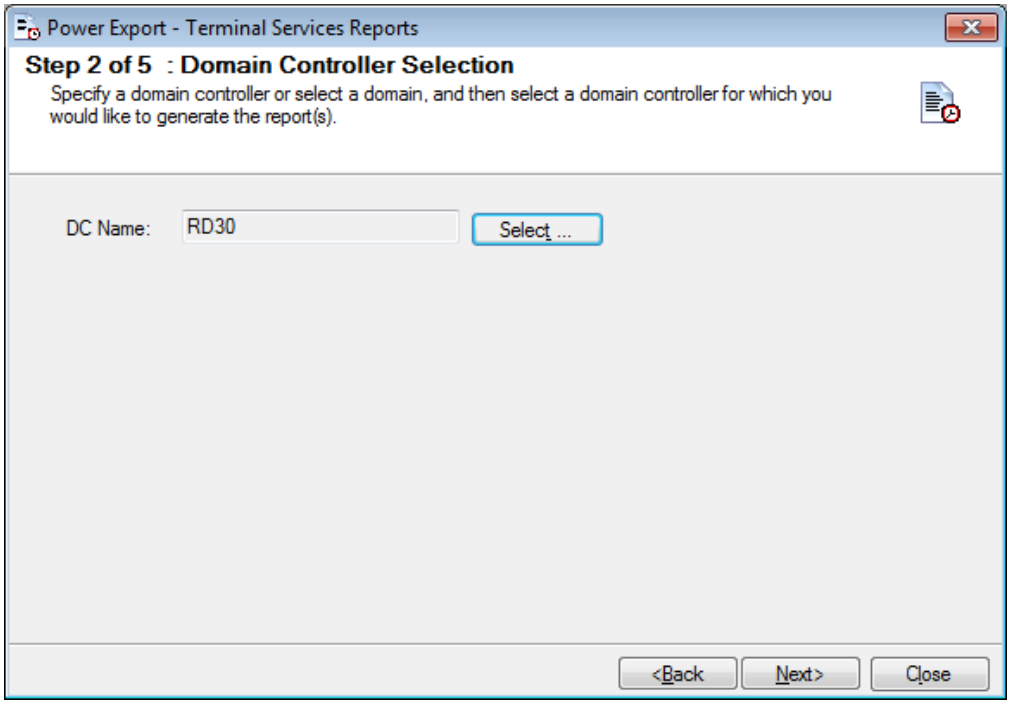
option under Power Export. This will bring up the Power Export Wizard.

Step 1: Report Selection


Power Export - Terminal Services Reports
Step 1 of 5 : Report Selection
Select the desired report to proceed.
Terminal Services Reports
<Back
Next>
Close

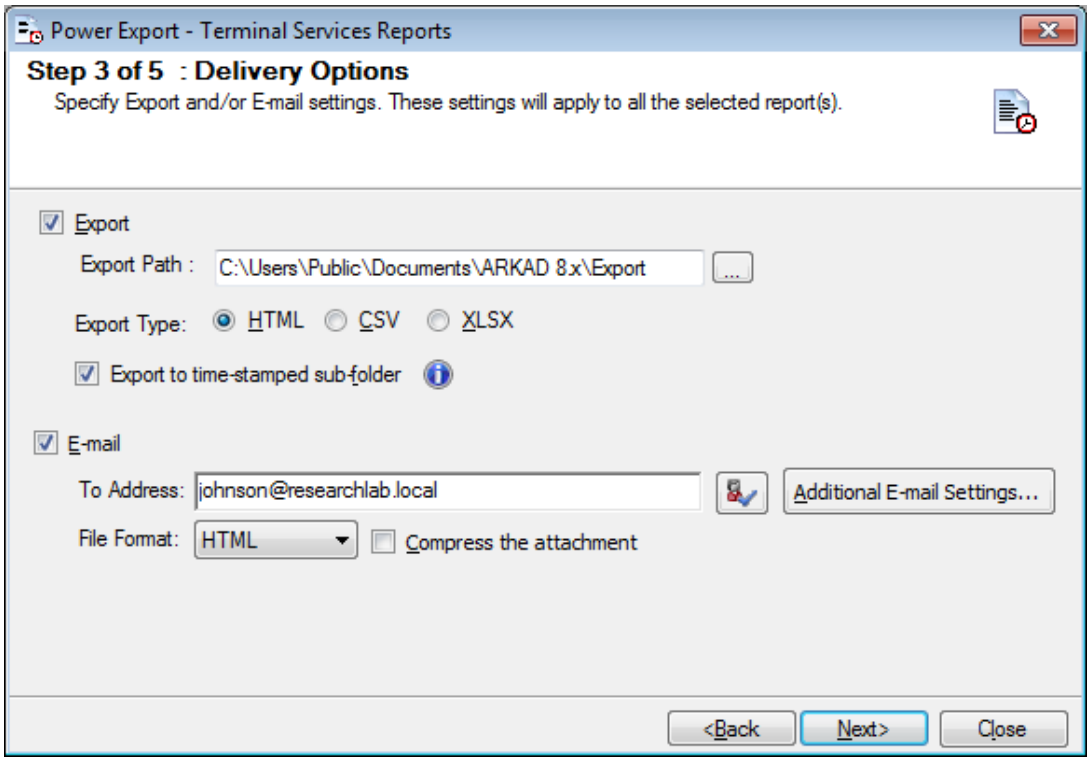
1) Select the report named **Terminal Services Reports.**
2) Click **Next** to proceed to the next step. You may Click **Back** button anytime to come back to a previous step.

Step 2: Domain Controller Selection


Power Export - Terminal Services Reports
Step 2 of 5 : Domain Controller Selection
Specify a domain controller or select a domain, and then select a domain controller for which you would like to generate the report(s).
DC Name:
RD30
Select ...
<Back
Next>
Close

1) Specify a domain controller for which you want to generate the selected custom report. Click Select button to specify a domain controller. The Connection Manager will be displayed which will allow you to specify a domain controller
2) Click **Next** to proceed to the next Step.

Step 3: Export/Email Options



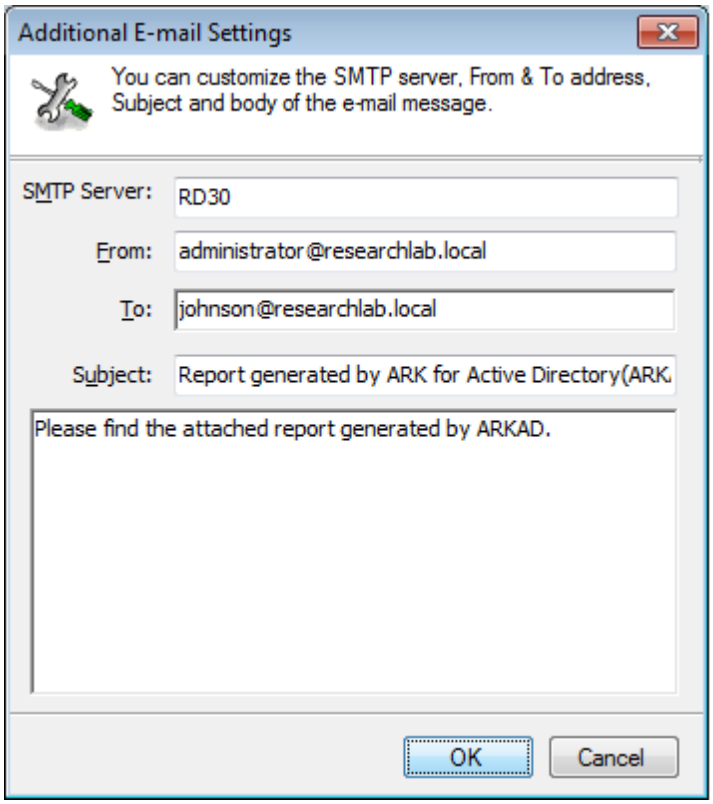
1) Change the Export or Email settings as necessary.

2) Use Browse button to change the export path.

3) The export path refers to the destination location where the output file generated should be stored. By default, for each task, a sub-folder with the task name will be created under the specified export path. All selected reports will be exported to a time-stamped folder, in the format "yyyy-mm-dd hh.mm.ss", under the task name folder. If you want to export to the specified folder instead, then click to clear "Export to time-stamped sub-folder" option.

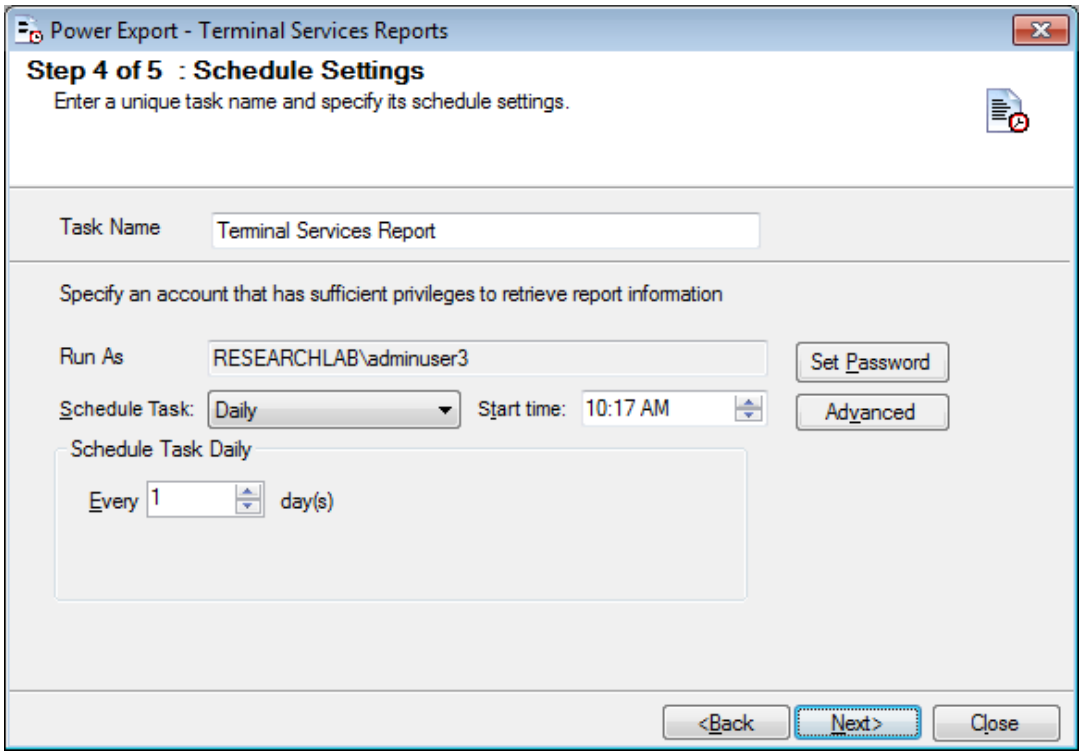
NOTE: Clearing the "Export to time-stamped sub-folder" option will overwrite existing files, if any, in the specified export path.

4) Click **Additional E-mail Settings** button to specify optional e-mail settings as shown below:



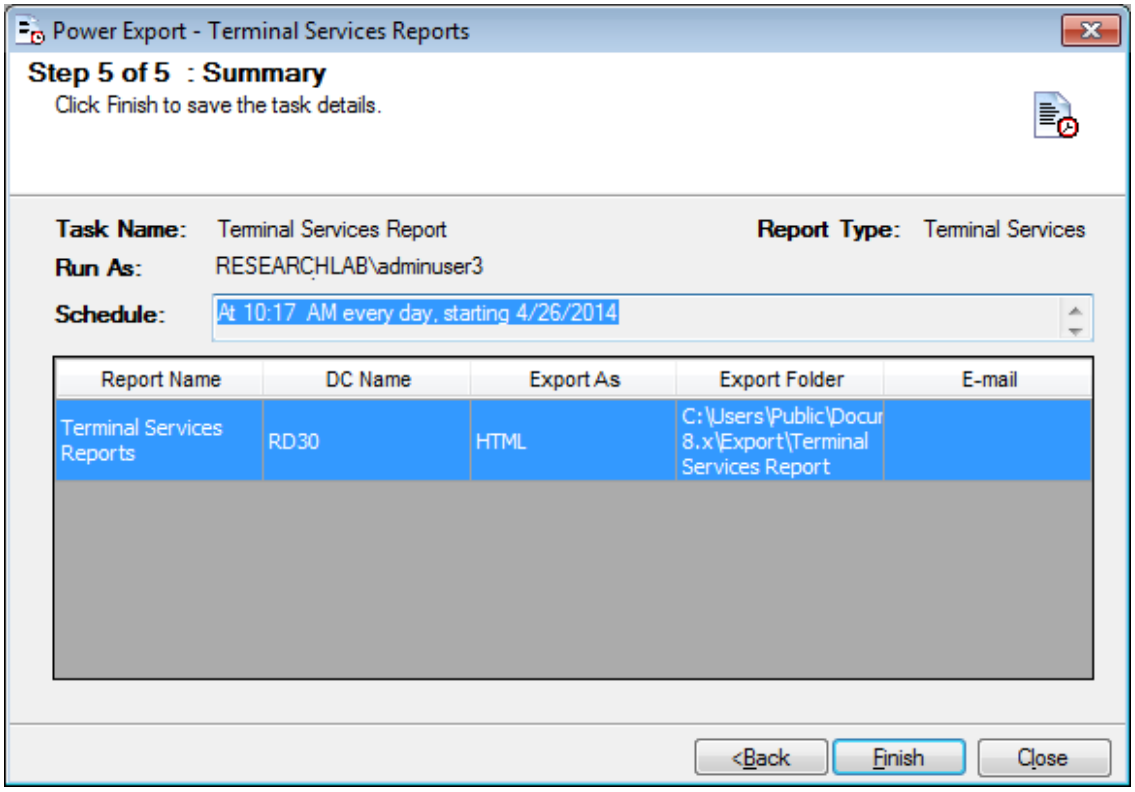
5) Click **Next** to Proceed to the Next Step.

Step 4: Schedule Settings



1) Enter a unique name for the task.
2) The task will run on currently logged on user and set password for the currently logged on user.
3) Change the task schedule settings as required.
4) Click **Next** to proceed to the next and final step.

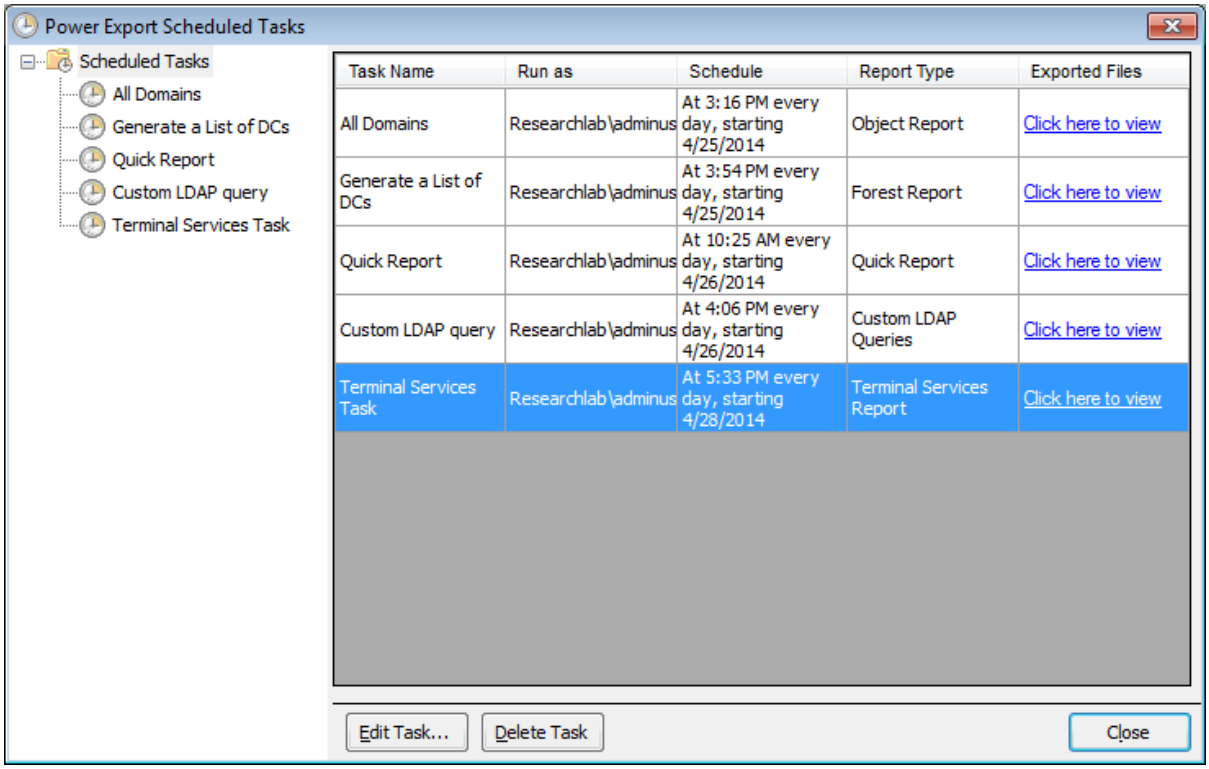
Step 5: Summary



1) This step displays the summary information of the task.

2) Click **Finish** to save the task details.

3) The task will be added to Windows Schedule Tasks and will be displayed in the Scheduled Tasks Manager Window as shown below:

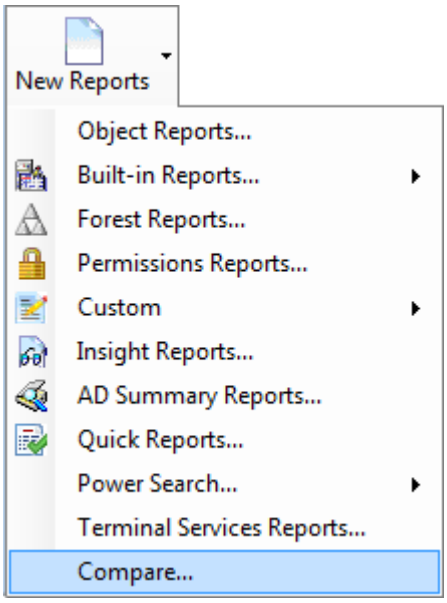


Chapter 15

15 Compare Reports

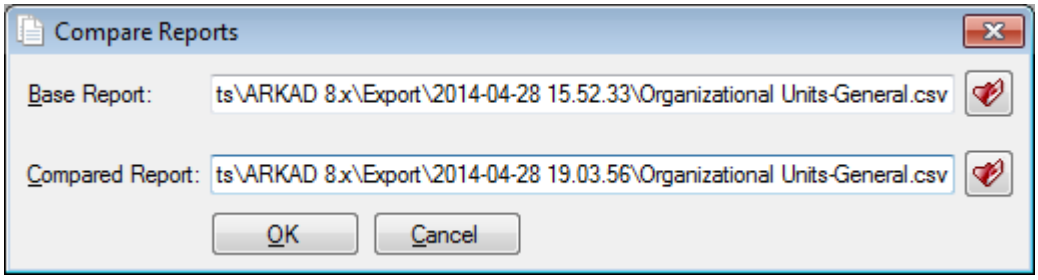
15.1 How to Compare Reports?

The Compare Reports is a powerful feature that allows you to compare reports generated using ARKAD. You can select two HTML, XLSX and CSV formatted reports generated in a different time period for comparison.

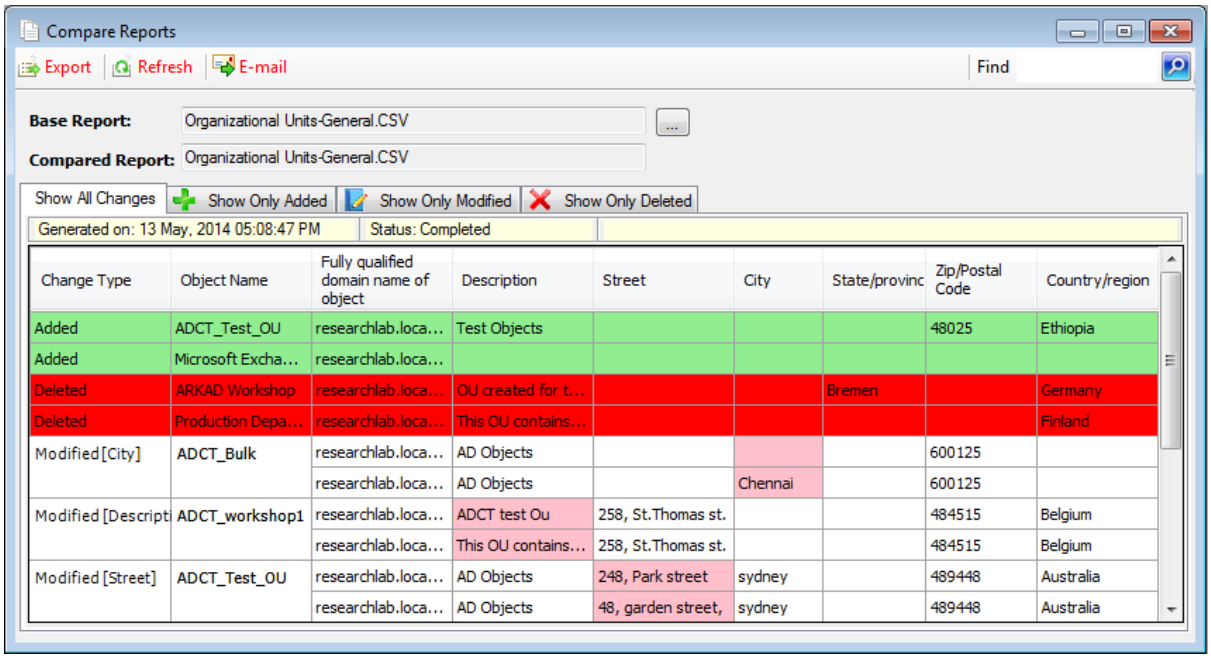


To launch 'Compare Reports' selection window, click menu in the toolbar. The 'Compare Reports' selection window will appear as shown below:

- Specify the Base Report and Compared Report for which you want to view the difference.
- Click Ok button to begin comparison.



Once the data comparison process is complete, the report would be generated in a report window as shown below:



Change Type	Object Name	Fully qualified domain name of object	Description	Street	City	State/provinc	Zip/Postal Code	Country/region
Added	ADCT_Test_OU	researchlab.loca...	Test Objects				48025	Ethiopia
Added	Microsoft Excha...	researchlab.loca...						
Deleted	ARKAD Workshop	researchlab.loca...	OU created for t...			Bremen		Germany
Deleted	Production Depa...	researchlab.loca...	This OU contains...					Finland
Modified [City]	ADCT_Bulk	researchlab.loca...	AD Objects				600125	
		researchlab.loca...	AD Objects		Chennai		600125	
Modified [Descripti	ADCT_workshop1	researchlab.loca...	ADCT test Ou	258, St.Thomas st.			484515	Belgium
		researchlab.loca...	This OU contains...	258, St.Thomas st.			484515	Belgium
Modified [Street]	ADCT_Test_OU	researchlab.loca...	AD Objects	248, Park street	sydney		489448	Australia
		researchlab.loca...	AD Objects	48, garden street,	sydney		489448	Australia

You can also click Show All Changes, Show Only Added, Show Only Modified and Show Only Deleted tabs to view the list of all changes, added, edited and deleted changes.

Chapter 16

16 References

16.1 Troubleshooting

If and when a problem arises, please forward the following information to support@vyapin.com to revert back to you with a solution.

Error Log File-

E.g., <*Application Data Folder*>\ARKAD 8.x\ARKADErrorLog.log

The <*Application Data Folder*> is the common location where ARKAD settings will be stored in the computer running ARKAD application. The <*Application Data Folder*> can be found from the **Help -> About** screen. The default path of <*Application Data Folder*> is as follows:

a) Windows XP, Windows 2003- C:\Documents and Settings\All Users\Documents
b) Windows 8, Windows 7, Windows Vista, Windows 2008 - C:\Users\Public\Documents

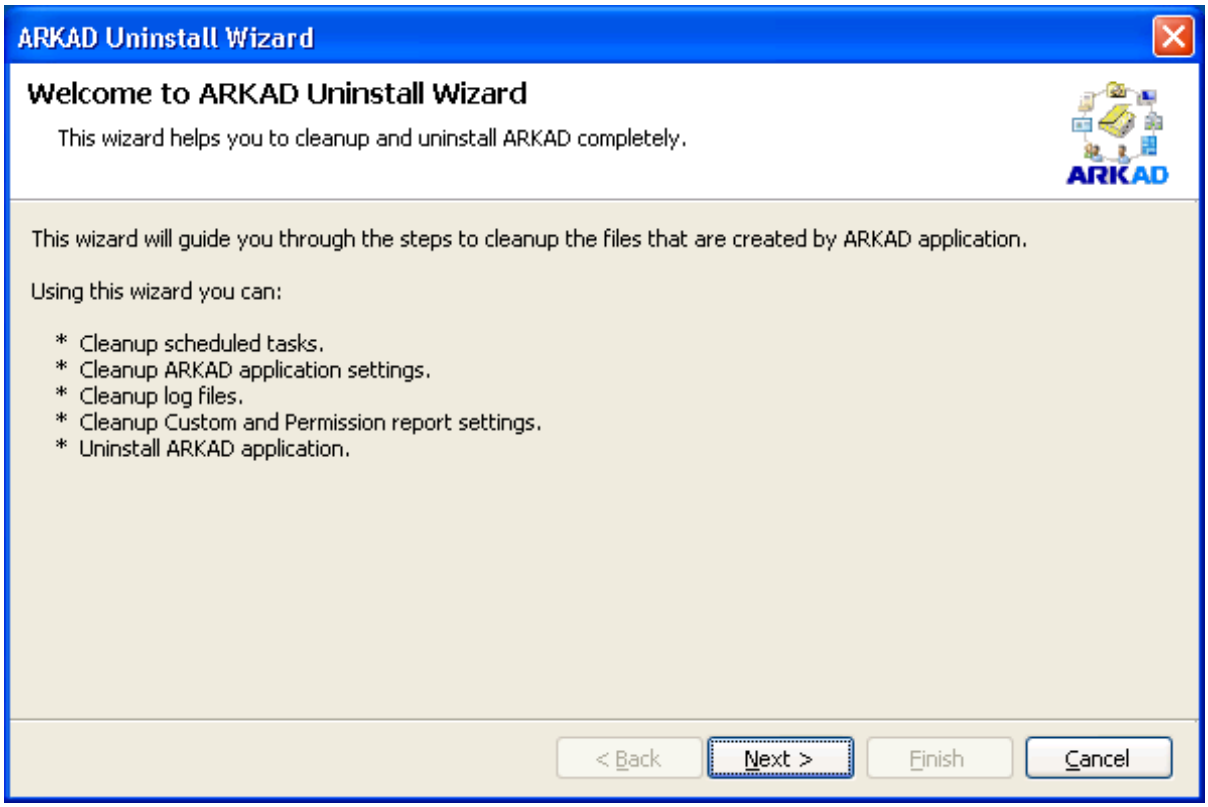
16.2 How to Uninstall ARKAD?

When you ***uninstall*** ARKAD through Control Panel - Add / Remove Programs applet, *Windows Installer program* will remove only the application files from your computer. But, the application related files created by ARKAD remain in the computer. In order to *remove* ARKAD worker files ***completely,*** the ***uninstall wizard*** provides a set of ***clean up*** options to perform the clean-up operation based your selection.

Use this wizard to clean up the files that are created by ARKAD application selectively and uninstall ARKAD completely from the computer.

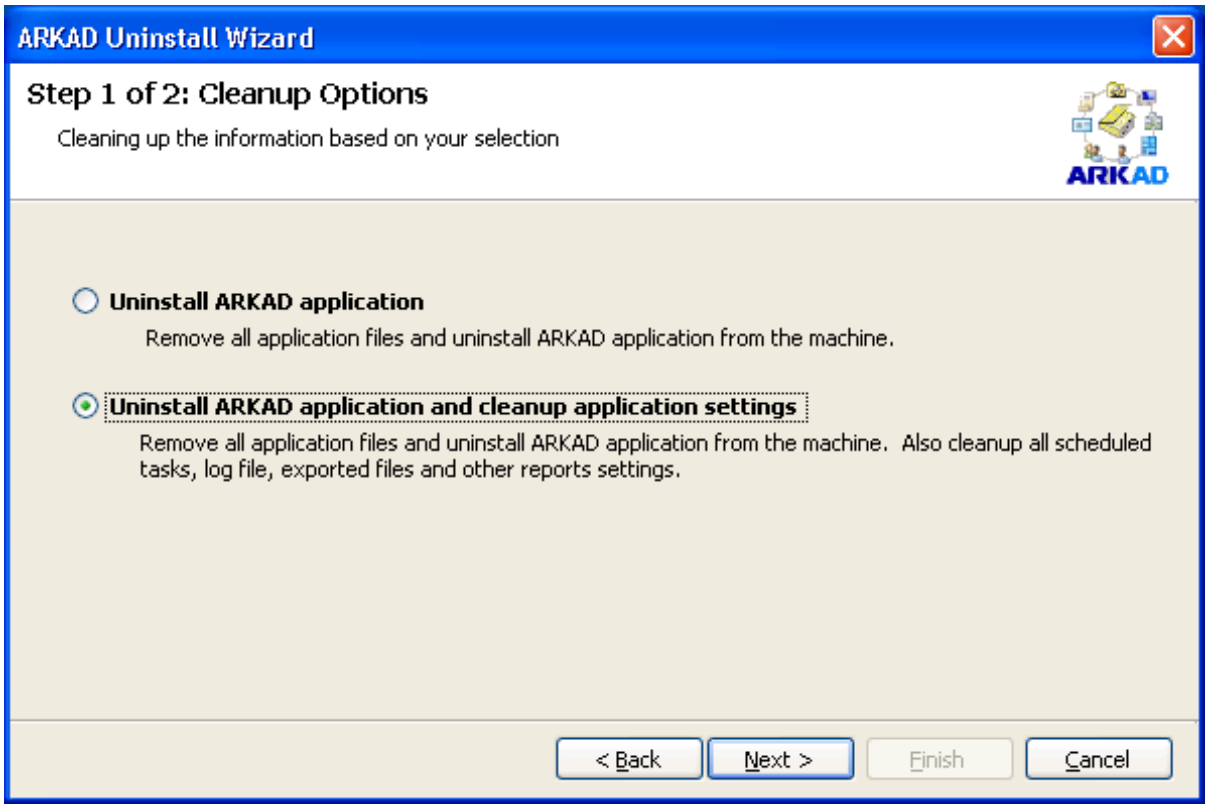
1) **Launch** the **uninstall wizard** by clicking *Start -> Programs -> Admin Report Kit for Active Directory v8.x -> Uninstall ARKAD v8.5*

The ARKAD ***Uninstall Wizard*** dialog will be shown as below:


ARKAD Uninstall Wizard
Welcome to ARKAD Uninstall Wizard
This wizard helps you to cleanup and uninstall ARKAD completely.
ARKAD
This wizard will guide you through the steps to cleanup the files that are created by ARKAD application.
Using this wizard you can:
* Cleanup scheduled tasks.
* Cleanup ARKAD application settings.
* Cleanup log files.
* Cleanup Custom and Permission report settings.
* Uninstall ARKAD application.
< Back
Next >
Finish
Cancel

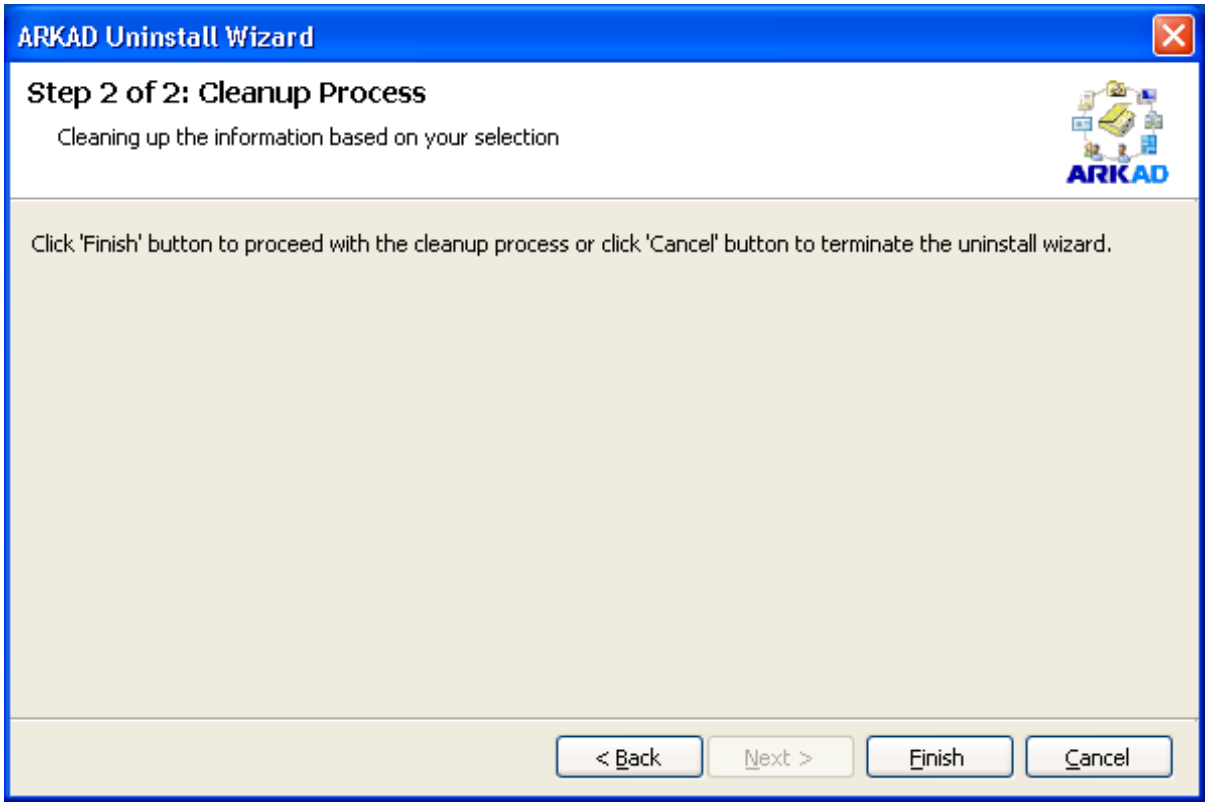
Click ***Next*** to proceed.

2) ***Select*** required ***clean up options*** as shown below:


ARKAD Uninstall Wizard
Step 1 of 2: Cleanup Options
Cleaning up the information based on your selection
ARKAD
Uninstall ARKAD application
Remove all application files and uninstall ARKAD application from the machine.
Uninstall ARKAD application and cleanup application settings
Remove all application files and uninstall ARKAD application from the machine. Also cleanup all scheduled tasks, log file, exported files and other reports settings.
< Back
Next >
Finish
Cancel

Click ***Next*** to proceed.

3) ***Confirm*** the ***cleanup*** and/or ***uninstall process.***


ARKAD Uninstall Wizard
Step 2 of 2: Cleanup Process
Cleaning up the information based on your selection
ARKAD
Click 'Finish' button to proceed with the cleanup process or click 'Cancel' button to terminate the uninstall wizard.
< Back
Next >
Finish
Cancel

4) *Click* ***Finish*** to run *cleanup and/or uninstall process*. *Click* ***Cancel*** to close the wizard.

5) Once the file cleanup process is ***complete***, the *uninstall wizard* will automatically run *Windows Installer* program to *remove* ARKAD application from the computer.

17 Index

About Admin Report Kit for Active Directory (ARKAD, 1

About Built-in Reports, 107

About Custom LDAP Queries, 148

About Custom Reports, 135

About Forest Reports, 117

About Insight Reports, 161

About Permissions Reports, 120

About Power Export, 202

About Power Search, 182

About Quick Reports, 105

Access Control Entry, 185

Access Denied, 89

Account expiration date, 61

Account is sensitive and cannot be delegated, 61

Account is trusted for delegation, 61

'Account Picker', 189

Accounts Selection, 188, 219

'ACE type', 185

activate the software., 6

Active Directory, 2, 55, 105, 107, 157, 158, 161, 182, 183, 264

AD Summary reports, 157

AD Summary Reports, 157, 203

Additional E-mail Settings, 247, 253

ARKAD, 66, 90, 105, 113, 117, 120, 123, 130, 135, 161, 202, 204, 264, 266

ARKAD application, 264, 266

Built-in Object Reports, 107, 203

Built-in reports, 107

Built-in Reports, 107, 108, 111

Built-in Security Reports, 107

Built-in Security Reports, 203

Computer Accounts, 54, 105, 157, 159, 161, 166, 169, 170

'Computer Accounts' node, 159

Computer Accounts Reports, 54

Computer Accounts., 54, 105, 166, 169, 170

Computer configuration enabled,, 90

Computer configuration version, 90

Computer name (pre-Windows 2000), 54

Configure Directory Server, 9

Connection Manager, 48, 54, 60, 69, 74, 79, 83, 90, 95, 97, 100, 106, 110, 113, 118, 123, 130, 135, 143, 157,

162, 166, 171, 177, 207, 214, 220, 225, 230, 235, 245, 251

Contact report, 74

Container Selection, 114, 124, 218

'Containers to search', 187

Create a new Custom Report, 145, 146

credential, 194, 195

Current USN, 49, 56, 64, 72, 77, 80, 102

Custom LDAP Query Reports, 148

Custom Reports, 135, 142, 145, 146, 203, 205

Custom Reports Wizard, 142

data collection process, 106, 110, 116, 119, 131, 144

Delegated Task, 51

Delete a custom report, 145, 146

Delete a Permissions Report, 132

Delete a task, 204

Delete Task, 205

DES encryption, 61, 176

Direct Reports, 63, 76

Domain, 157

domain controller, 48, 53, 54, 58, 60, 67, 69, 73, 74, 78, 82, 83, 90, 94, 95, 97, 99, 100, 104, 106, 110, 113, 118, 123, 130, 143, 157, 162, 166, 171, 177

Domain controller, 39

Domain Controller, 112, 122, 206, 213, 220, 225, 230, 235, 245, 251

domain controller name, 188

domain controllers, 169

Domain General Summary report, 158

domain name, 72, 73, 92, 134, 188

Domain Name, 114, 124

'Domain' node, 158

Domain Selection, 184

Edit an existing Custom Report, 145, 146

Edit an existing Permissions report, 133

Edit an existing task, 204

Edit Task, 205

Effective PSO, 67

Employee ID, 60, 67

Employee Number, 60, 67

Employee Type,, 67

Error Log File, 263

existing Permissions Report, 132

explicit, 185

export path., 202, 208, 214, 221, 226, 231, 236, 246, 252

Export/Email Options, 208, 214, 221, 226, 231, 236, 246, 252

Exported Files, 204, 205

Field Selection, 115, 125, 137, 219

File System Path, 89

Foreign Security Principals, 79, 158

Foreign Security Principals report, 79

Forest Reports, 117, 118, 203

FQDN, 63, 70, 71, 80, 91, 97, 102

Fully qualified domain name, 39, 40, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65, 66, 67, 69, 70, 71, 72, 74, 75, 76, 77, 78, 79, 80, 81, 90, 91, 92, 93, 97, 98, 99, 100, 101, 102, 103

General Summary report, 158, 159

Generate a custom report, 145

Generate a permissions report, 134

Generate a Permissions Report, 133

Global Groups, 159

GPO Name, 89

Group Policy, 51, 90, 117

Groups General Summary report, 159

Groups report, 69

GUID Name, 89

House Identifier, 67

How to Activate the Software?, 6

How to Add Server to Connection Manager?, 11

How to Add/Remove Columns?, 25

How to Configure Profile Manager?, 36

How to Configure SMTP Server?, 35

How to Create Custom LDAP Query Report?, 148

How to create Custom Reports?, 135

How to create Permissions Reports?, 120

How to Delete Custom LDAP Query Report?, 156

How to Edit Server in Connection Manager?, 14

How to E-mail data?, 21

How to Export Data?, 20

How to Find Data in a Report?, 18

How to generate AD Summary Reports?, 157

How to Generate Built-in Object Reports?, 108

How to Generate Built-in Security Reports?, 111

How to Generate Custom LDAP Query Report?, 154

How to generate Custom Reports?, 142

How to generate Forest Reports?, 117

How to generate Permissions Reports?, 129

How to Generate Power Search Reports?, 196

How to generate Quick Reports?, 106

How to Manage Custom LDAP Query Report?, 155

How to Manage Custom Reports?, 145

How to Manage Permissions Reports?, 132

How to Manage Power Search Reports?, 192

How to Perform a New Account Search?, 197

How to Perform a New Power Search?, 184

How to read the Report Status label?, 33

How to refresh data?, 25

How to Uninstall ARKAD?, 264

How to Use Advanced Filter?, 27

How to use ARKAD effectively?, 9

How to use Quick Filter?, 31

How to view Computer Accounts Reports?, 54

How to view Contacts Reports?, 74

How to view Domain Reports?, 38

How to view Foreign Security Principals?, 79

How to view Group Policy Object Reports?, 90

How to view Groups Reports?, 69

How to view Insight Report for Computer Accounts?, 166

How to view Insight Report for Groups?, 177

How to view Insight Report for Organizational Units?, 162

How to view Insight Report for Users?, 171

How to view Organizational Unit Reports, 48

How to view Password Settings Objects Reports?, 100

How to View Properties of Server in Connection Manager?, 17

How to view RSoP Reports?, 83

How to view Sites Reports?, 44

How to view Starter GPOs Reports?, 95

How to view Users Reports?, 60

How to view WMI Filter Reports?, 97

Insight Reports, 161

interactive logon, 61, 175

IP Phone Number, 62, 75

Items Reported, 165, 169, 173, 179

Kerberos, 61, 176

Last known parent, 52, 53, 58, 67, 73, 78, 82, 94, 99, 104

Last Logon, 54, 58, 66

Launch Connection Manager, 9

Linked GPO, 91, 97

list of accounts, 188

Logon Script, 62

Maximum Password Age, 101

Member Of, Primary group, 76

Membership Group, 63, 71, 80

Membership Group SID, 63, 71, 80

Minimum Password Age, 101

Minimum Password Length, 101

network planning personnel, 5

new Permissions Report, 132

New Search, 184

Number of computers running Windows XP Professional, 170

Object Links, 51

Object Name, 40, 48, 49, 50, 51, 52, 54, 55, 56, 57, 58, 60, 61, 62, 63, 64, 65, 66, 67, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 97, 98, 99, 100, 101, 102, 103, 104

Object Reports, 38, 117, 135, 147, 203, 205

Object Selection, 112, 136

Operating System, 5, 55, 169, 170

Organizational Unit General report, 48

Organizational Units, 48, 157, 158, 161, 162, 165

Organizational Units., 157, 162, 165

Original USN, 49, 56, 64, 72, 77, 80, 102

parameters, 161, 163, 164, 167, 172, 173, 178, 179, 212, 218, 219

Password expiration date, 66

Password Settings Objects, 100

Password Settings Objects., 100

Passwords applet, 12

permission inheritance, 185

Permission Selection, 185

permissions category, 185, 186

permissions report., 129

Permissions Reports, 120, 121, 129, 130, 132, 133, 203

Permissions Reports Wizard, 130

Power Export, 117, 202, 203, 206, 211, 217, 224, 229, 234, 244, 250

Power Search, 182, 183, 184, 191, 192, 193, 194, 195, 196

Power Search Wizard, 184

preauthentication, 61

Email settings, 208, 214, 221, 226, 231, 236, 246, 252

Profile Path, 62

PSO Description, 66

Quick Reports, 105

References, 263

Refresh Data, 167

Remote Access Permission, 64

Report Criteria, 140

Report Selection, 108, 111, 206, 211, 217, 224, 229, 234, 244, 250

Resultant PSO,, 66

RSoP report, 83

'Save search', 191

Schedule AD Summary Reports, 244

Schedule Built-in Object Reports, 211

Schedule Built-in Security Reports, 217

Schedule Custom LDAP Queries Reports, 239

Schedule Custom Reports, 234

Schedule Forest Reports, 224

Schedule Object Reports, 206

Schedule Permissions Reports, 229

Schedule Quick Reports, 250

Schedule Settings, 209, 215, 222, 227, 232, 237, 248, 253

Scheduled Tasks, 202, 204, 205, 210, 216, 223, 228, 233, 238, 249, 255

Scheduled Tasks Manager, 204

schema definition, 183

Scope Selection, 186

Server Selection, 110

set of accounts, 188

SID, 58, 60, 61, 62, 63, 64, 65, 66, 67, 69, 70, 71, 72, 73, 79, 80, 81, 82, 92, 96

Smart card, 61, 175

Source GPO, 83, 84, 85, 86, 87, 88

Specify Report Parameters, 212, 218

Summary, 157, 158, 159, 160, 161, 163, 164, 167, 168, 172, 173, 178, 179, 203, 210, 216, 228, 233, 238, 248, 254

System Administrators, 5

System requirements, 5

Systems management personnel, 5

Technical Support, 8

Total no of Computers running Windows XP Professional, 159

Troubleshooting, 263

Trust computer for delegation, 54

uninstall ARKAD, 264

Uninstall Wizard, 264

Unique ID, 90, 91, 92, 93, 95, 96, 97, 98, 99

Universal Groups, 159

User configuration enabled, 90

User configuration version, 90

user credential, 188

User logon name, 61

Users report, 60

View Details, 130, 133, 143, 146, 164, 168, 173, 179

View exported files, 204

View fields defined for a custom report, 145, 146

View Options, 163, 167, 172, 178

View settings for a permissions report, 133

Web Page Address, 60, 74

Who can use ARKAD?, 5

Windows 7, 159

Windows Installer, 264, 266

Windows network product developers, 5

Windows Server 2003, 53, 58, 67, 73, 78, 82, 83, 94, 99, 104, 159, 170

WMI Filter, 89, 90

WMI Filters., 97, 114, 124